S. HRG. 111–664

CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM
AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED ELEVENTH CONGRESS

SECOND

NOVEMBER 17, 2009

Serial No. J–111–62

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

61–662 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

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00001 Fmt 5011 Sfmt 5011 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

CONTENTS

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin	JEFF SESSIONS, Alabama
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
RUSSELL D. FEINGOLD, Wisconsin	CHARLES E. GRASSLEY, Iowa
CHARLES E. SCHUMER, New York	JON KYL, Arizona
RICHARD J. DURBIN, Illinois	LINDSEY GRAHAM, South Carolina
BENJAMIN L. CARDIN, Maryland	JOHN CORNYN, Texas
SHELDON WHITEHOUSE, Rhode Island	TOM COBURN, Oklahoma
AMY KLOBUCHAR, Minnesota	
EDWARD E. KAUFMAN, Delaware	
ARLEN SPECTER, Pennsylvania	
AL FRANKEN, Minnesota	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
MATT MINER, *Republican Chief Counsel*

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

BENJAMIN L. CARDIN, Maryland, *Chairman*

HERB KOHL, Wisconsin	JON KYL, Arizona
DIANNE FEINSTEIN, California	ORRIN G. HATCH, Utah
CHARLES E. SCHUMER, New York	JEFF SESSIONS, Alabama
RICHARD J. DURBIN, Illinois	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	TOM COBURN, Oklahoma
EDWARD E. KAUFMAN, Delaware	

BILL VAN HORNE, *Democratic Chief Counsel*
STEPHEN HIGGINS, *Republican Chief Counsel*

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00002 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS AND ANSWERS

SUBMISSIONS FOR THE RECORD

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00003 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00004 Fmt 5904 Sfmt 5904 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE

TUESDAY, NOVEMBER 17, 2009

U.S. SENATE,
SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Benjamin L. Cardin, Chairman of the Subcommittee, presiding.

Present: Senators Cardin, Kohl, Feinstein, Schumer, Durbin, Kaufman, Kyl, Hatch, Sessions, Cornyn, and Coburn.

OPENING STATEMENT OF HON. BENJAMIN L. CARDIN, A U.S. SENATOR FROM THE STATE OF MARYLAND

Chairman CARDIN. The Subcommittee will come to order, the Subcommittee on Terrorism and Homeland Security. Our topic today is "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace."

I must tell you I think this is a very sobering subject. As we have seen the advancement of technology, we have also seen the enhanced risks against our homeland security.

On November the 8th, "60 Minutes" did an expose on what many of us have feared in the development of cyberspace. It showed that the technology advancement has indeed made our Nation at greater risk. We are vulnerable. We are vulnerable from terrorist attacks against our country using cyberspace. They can steal sensitive information which can compromise our national security. They can, more frighteningly, alter data which is used to run critical infrastructure for this country, information systems, attacking our infrastructure, whether it is our energy grid or whether it is our financial institutions, all causing significant damage to the United States. It can compromise our military assets which are used to defend our Nation.

And it is not just Government that is at risk. It is the private sector also at risk. Financial information can be used to obtain illegal funds. It is the modern-day bank robbers, but they do not have to use hoods and masks and guns and go into banks. They can invade our financial institutions and steal money from the depositors. Identity theft is much more at risk because of technology advancements.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00005 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

It is not only financial information. It is sensitive information such as health records, and it can be used to extort funds from people in our country.

The Government has a responsibility to protect our Government and its citizens from these attacks, from those who might misuse cyberspace. Also, Government has a responsibility that in its countermeasures it also strikes the right balance between getting the information necessary to protect us from cyber attacks, but also protect the privacy of Americans as well.

President Obama, shortly after taking office, undertook a comprehensive clean-slate review to assess U.S. policies and structures for cybersecurity. Now, some of the conclusions are of interest to this Committee, and I think some are disturbing. One of the conclusions of that review showed that the Federal Government is not organized to address the growing problems of cybersecurity; that there are overlapping agencies' responsibilities; this Nation is at a crossroads; the status quo is no longer acceptable; and that the national dialog on cybersecurity must begin today. I agree with that conclusion.

The study also pointed out the need to appoint a cybersecurity policy officer responsible for coordination of the national cybersecurity policies and activities. In other words, we need a point person that has that responsibility. I know a lot of agencies have this responsibility, but they are at cross-purposes and at times conflicting. The report also indicated we need to designate a privacy and civil liberties official to the National Security Council Cyber Security Directorate.

A point that we certainly will be taking up in this hearing is how do we enhance and protect the civil liberties of the people of this Nation.

The bottom line is that we need to coordinate Government efforts also using the private sector to make sure we are as effective as possible to protect our Nation against this vulnerability.

Well, I am pleased that at today's hearing we have two panels. First we have a panel of Government experts who are responsible for cybersecurity in this country and developing the policies for cybersecurity in this country. And then in the second panel we will hear from the private sector as to how we can coordinate both the private and public sector.

Senator Kyl will be joining us shortly. I notified his staff that I would start immediately at 10 o'clock because there are scheduled votes on the floor of the Senate at around 11:15 to 11:30. Now, in the Senate we do not always adhere to when the scheduled votes are scheduled, but in an effort to try to make sure that we have the maximum time available for asking questions, we started promptly at 10 o'clock.

Our first panel consists of four Government witnesses: James Baker, who was sworn in as the Assistant Deputy Attorney General at the United States Department of Justice in July of 2009. He has worked on numerous national security matters during his career. As a former Federal prosecutor, he worked on all aspects of national security investigations and prosecutions, including particularly the Foreign Intelligence Surveillance Act, FISA, during

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00006 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

his 17-year career as an official at the United States Department of Justice from 1990 to 2007.

Phil Reitinger was appointed to serve as Deputy Under Secretary for the National Protection and Programs Directorate on March 11, 2009. In this role, Mr. Reitinger leads the Homeland Security Department's integrated efforts to reduce risks across physical and cyber infrastructure. On June 1, 2009, he also became the Director of the National Cyber Security Center, which is charged with enhancing the security of Federal networks and systems by collecting, analyzing, integrating, and sharing information among interagency partners.

Richard Schaeffer is the Information Assurance Director at the National Security Agency. He is responsible for the availability of products, services, technologies, and standards for protecting and defending our Nation's critical infrastructure systems from adversaries in cyberspace.

And then Steven Chabinsky serves as the Deputy Assistant Director within the FBI's Cyber Division. Mr. Chabinsky recently returned to the FBI after completing a joint duty assignment with the Office of the Director of National Intelligence, where he served as Assistant Director of National Intelligence for Cyber, the Chair of the National Cyber Study Group, and the Director of the Joint Interagency Cyber Task Force.

Before calling on the witnesses, let me yield to Senator Kyl, the Ranking Republican on the Subcommittee.

STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator KYL. Mr. Chairman, thank you. I am sorry I missed most of your opening statement, the most important part of the hearing, but I am sure I will get a copy of that and review it. I want to thank the witnesses as well. We have been talking about this hearing for some time. I really applaud you for being able to put together a great panel for us today.

The Federal Government increasingly relies on interconnected information systems for its crucial day-to-day operations, and these systems are ever more subject to cyber crime as well as cyber espionage.

I am concerned in particular about China, a growing threat to U.S. cybersecurity. In a report published last month by the U.S.-China Economic and Security Review Commission, here is what was said: "Increasingly, Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict. China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. Government."

And then the report goes on to say, "In a conflict with the U.S., China will likely use its computer network operations capabilities to attack unclassified DOD and civilian contractor logistics networks in the continental United States and allied countries in the Asia-Pacific Region. The stated goal in targeting these systems is to delay U.S. deployments and impact combat effectiveness of troops already in theater." Just one example of the way that an attack could occur.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

Obviously, we do not think the Chinese forces could defeat ours head on head, so they seek another method to gain advantage. And in my view, the U.S. is not adequately countering this serious and growing threat.

During a recent interview on a news program, "60 Minutes," the Director of Technology and Public Policy Program at the Center for Strategic and International Studies said that the U.S. faced a so-called electronic Pearl Harbor in 2007 when an unknown foreign power broke into the computer systems at the Departments of Defense, State, Commerce, and Energy, and probably NASA, and downloaded the equivalent of a Library of Congress worth of information.

During the same news segment, when asked about the possibility that penetrations into U.S. systems had left behind malicious software that could enable future attacks, former Director of National Intelligence Mike McConnell responded, "I would be shocked if we were in a situation where the tools and capabilities and techniques had not been left in U.S. computer and information systems." So, obviously, he is concerned as well.

As with the threat from terrorism, our Government must use all tools available to address this threat and protect our citizens and way of life. A key challenge in this regard is balancing the privacy of U.S. citizens.

Representatives of the departments that are in charge of addressing cybersecurity vulnerabilities are assembled before us today, and I look forward to hearing how they are planning to get ahead of this growing cyber threat. Again, thank you for your considerable interest in the subject.

Chairman CARDIN. Thank you, Senator Kyl. It has been a pleasure working with you on this issue. This is an area of great interest to every Member of the Senate, and it is given a high priority by both you and me and this Subcommittee.

With that, I would ask our witnesses first to stand in order to administer the oath, and then we will start with their testimony. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. BAKER. I do.

Mr. REITINGER. I do.

Mr. SCHAEFFER. I do.

Mr. CHABINSKY. I do.

Chairman CARDIN. Thank you. Mr. Baker, we are pleased to hear from you. And, by the way, all of your full statements will be made part of the record, and you may proceed as you wish.

STATEMENT OF JAMES A. BAKER, ASSOCIATE DEPUTY ATTORNEY GENERAL, OFFICE OF THE DEPUTY ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. BAKER. Thank you, Mr. Chairman, members of the Subcommittee, and members of the Committee. I appreciate this opportunity to discuss the critical issue of protecting the Nation from cybersecurity threats while ensuring the protection of civil liberties and privacy, as has been mentioned already. I have submitted a

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00008 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

lengthy statement for the record, and I will not repeat that here, but I would just like to make a few brief points.

First of all, the Department of Justice is key player in the cybersecurity arena. Among other things, we provide legal advice and guidance on a range of cybersecurity activities to other Federal entities. Our objective is to ensure full use of available legal authorities and strict adherence to the law, including civil liberties and privacy protections. In addition, we assist in the development of cybersecurity policy. DOJ is a full participant in the interagency policy process.

Further, we collect information and conduct investigations regarding cybersecurity threats in partnership with law enforcement and intelligence agencies. Importantly, obviously, we prosecute cyber criminals in Federal court. We use the full range of available criminal statutes to seek the maximum penalties against cyber criminals.

Further, we train investigators and prosecutors around the country to make sure that we have knowledgeable officials ready to respond to the cyber threats of today. We engage with our foreign law enforcement partners to deny safe havens to cyber criminals and to bring them to justice wherever it may be most advantageous.

If I could just quickly highlight one of the functions of the Department of Justice in the FBI, which will be talked about later, the NCIJTF, which is the National Cyber Investigative Joint Task Force. NCIJTF is in my experience a very forward-looking organization that engages in robust information sharing and coordination across Federal agencies. At the same time, they have a strong awareness of the need to adhere to applicable laws that govern the collection and use of information. They certainly recognize that they have a long way to go, but in my view, they embody the significant changes that the FBI has made over the past 5 years.

Now, if I could turn briefly to the legal regime that governs cyber activities. There is a complex set of legal authorities that governs in this area. The Constitution, Federal statutes, State law, foreign law, international law—all have an impact in this area. These laws were developed over time in response to legal, policy, and technological developments.

The legal regime currently enables law enforcement and intelligence officials to obtain authorizations to collect vital information through electronic surveillance and other collection means. The legal authorities require strict adherence to a variety of civil liberties and privacy protections that are well understood by investigative agents.

However, the evolution of technology, our dependence on technology, and our adversaries' exploitation of vulnerabilities in that technology raises the question of whether our statutes are adequate to address the cyber threats of today and at the same time protect privacy and civil liberties. The administration is prepared to partner with Congress to ensure that adequate laws, policies, and resources are available to support the U.S. cybersecurity-related missions.

Further, because most of the cyber infrastructure is in private hands, we must also consult with industry in this important effort.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00009 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

As we move forward, it is critical that we proceed carefully so that we do not modify applicable law in a way that inadvertently harms important collection efforts or undermines existing requirements that are critical to the protection of civil liberties and legitimate privacy interests.

I would like to thank the Chairman and the Subcommittee for your leadership on this issue, and I look forward to your questions.

[The prepared statement of Mr. Baker appears as a submission for the record.]

Chairman CARDIN. Thank you very much for your testimony.

Mr. Reitinger.

STATEMENT OF PHILIP REITINGER, DEPUTY UNDER SECRETARY, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, DIRECTOR, NATIONAL CYBER SECURITY CENTER, U.S. DEPARTMENT OF HOMELAND SECURITY, WASHINGTON, DC

Mr. REITINGER. Thank you, sir. Chairman Cardin, Ranking Member Kyl, and members of the Committee and Subcommittee, thank you for the opportunity to be here today to talk to you about the growing threats that we face in cyberspace.

As I think the Committee and Subcommittee are aware, the threats are increasing. Your comments, Chairman, clearly indicate that. The skill level of attackers is rising across the spectrum from the most sophisticated attackers to the least sophisticated attackers. And, in fact, the most sophisticated attackers increasingly write high-quality tools that enable the least sophisticated attackers to launch very directed attacks without necessarily knowing that much.

At the same time, also as your comments point out, sir, we are depending more on these systems day to day, not just for communicating and doing work, but for operating our infrastructure and for the basic functions of our life.

As a result, as you point out, the status quo is simply not sufficient. We all need to up our game in Government and the private sector to increase the security and resiliency of our systems, but that is not our only goal. At the same time, we need to increase the competitiveness of our country so that we can maintain our lead going forward and we need to protect privacy by design. I would like to talk about some of our efforts in each of those areas.

To begin with, security. There is no silver-bullet solution here, sir. We are all working very hard across Government, but as Mr. Baker's comments indicate, this is going to take a broad set of efforts from the Government and the private sector. So we in the Department of Homeland Security and with our partners in Government and industry are working very hard to develop the right relationships to be able to be effective.

A recent announcement we have made in this space is the announcement of the National Cyber Security and Communications Integration Center, where we for the first time in the Department of Homeland Security, in direct response to advice we received from the private sector and from Congress through the Government Accountability Office, collocated the various operational watch centers we have for cybersecurity and communications in the same place.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00010 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

So our telecommunications watch capability, the National Coordinating Center, our IT security-based coordinating capability, US–CERT, and our cross-Government coordinating capability, the National Cyber Security Center, their watch components are all now located in the same space with appropriate liaisons from other Government agencies like the FBI so that they can breathe the same air, build trust, and collaborate effectively to respond to significant incidents that call for that level of cooperation.

Second, competitiveness. One of the things we need to do as a Nation is make sure that we are not only addressing the security issues we face now but are prepared to address them going forward. That means we need a bigger pool of cybersecurity experts to hire. I am trying in the Department of Homeland Security, in the National Cyber Security Division, to go from roughly 115 people on board at the end of the last fiscal year to about 260 by the end of the upcoming fiscal year. As I think those of you who know, that is a growth of over 50 percent, and it is a pretty heavy lift. In doing so, we will be competing with some of the other agencies you see up here and the people in the private sector. And unless we can grow that pool of people, that is going to be a zero-sum game. So, also with our partners in Government, we are working very hard to build the relationships, to build the techniques, and to build the programs that will build a pool of cybersecurity experts coming from our own universities that we will be able to be successful in the future, and I believe Mr. Schaeffer may talk a little bit more about that.

Let me then turn to privacy briefly. Privacy is absolutely essential. We are working very hard in this space, including building the processes, training, oversight mechanisms, and transparency, that we need to assure that our computer security efforts, our information assurance efforts, are compliant with and actually advance privacy rather than impair it. And we are working to support other administration efforts such as enhancing identity management strategies that are sensitive to privacy so that, going forward, we will be even more successful.

The one thing I would call out here as a key area for us is raising awareness because unless we can continue to raise the awareness of the American people and business interests, they are not going to be able to protect themselves. So during October, Cybersecurity Awareness Month, we made significant efforts to do that. I would be happy to talk more about that in the question-and-answer period if it is of interest to the Committee.

In conclusion, I would say that it is clear, I think, to all of us that cybersecurity is a team sport. We are collaborating very effectively across Government, and I look forward to the Committee's questions to explore more of these questions in detail. Thank you, sir.

[The prepared statement of Mr. Reitinger appears as a submission for the record.]

Chairman CARDIN. Thank you.

Mr. Schaeffer.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00011 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

STATEMENT OF RICHARD C. SCHAEFFER, JR., DIRECTOR, INFORMATION ASSURANCE DIRECTORATE, NATIONAL SECURITY AGENCY, U.S. DEPARTMENT OF DEFENSE, FORT MEADE, MARYLAND

Mr. SCHAEFFER. Thank you, sir. Good morning, Chairman Cardin, Ranking Member Kyl, and distinguished members of the Subcommittee. I appreciate the opportunity to be here today to talk briefly about the NSA's information assurance mission and its relationship to the work of the Department of Homeland Security and others concerned with helping operators of crucial information systems protect and defend their data systems and networks from hostile acts and other disruptive events.

Each day, ever more data and functions that are vital to the Nation are consigned to digital systems and complex interdependent networks. As Mr. Reitinger said, there are no silver bullets when it comes to cybersecurity. But, over time, increased awareness of cybersecurity issues, new standards, better education, expanding information sharing, more uniform practices, and improved technology can and will make a meaningful difference.

Many people who discuss this issue see only the challenges and, quite frankly, discuss them in ways in which the situation seems to be hopeless. I believe that that glass is half-full, and there are a number of steps that individuals and system owners and users can take to mitigate many of the threats of operating in cyberspace.

The NSA's information assurance mission focuses on protecting what National Security Directive 42 defines as national security systems. Those are systems that process, store, and transmit classified information or otherwise critical to military or intelligence activities. Historically, much of our work has been sponsored by and tailored for the Department of Defense. Today, national security systems are heavily dependent on commercial products and infrastructure or interconnect with systems that are. This creates new and significant common ground between defense and broader U.S. Government and homeland security needs. More and more we find that protecting national security systems demands teaming with public and private institutions to raise the information assurance level of products and services more broadly. If done correctly, this is a win-win situation that benefits the whole spectrum of information technology users, from warfighters and policymakers to Federal, State, local, and tribal governments, to the operators of critical infrastructure, and the Nation's most sensitive arteries of commerce.

In my statement for the record, which I submitted in advance, I used several recent specific examples of NSA's close and continued collaboration with Government organizations as well as our partners from industry and academia. For instance, the NSA and the National Institute of Standards and Technology have been working together for several years to characterize cyber vulnerabilities, threats, and countermeasures to provide practical cryptographic and cybersecurity guidance to both IT suppliers and consumers. Among other things, we have compiled and published security checklists for hardening computers and networks against a variety of threats. We have shaped and promoted standards that

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00012 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

enable information about computer vulnerabilities to be more easily catalogued and exchanged and ultimately the vulnerabilities themselves to be automatically patched. And we have begun studying how to extend our joint vulnerability management efforts to directly support compliance programs such as those associated with the Federal Information Security Management Act. All of this is unclassified and advances cybersecurity in general, from national security and other Government networks to critical infrastructure and other commercial or private systems.

The NSA partners similarly with the Department of Homeland Security. Earlier this year, we proudly announced the designation of 29 additional U.S. colleges and universities as National Centers of Academic Excellence in Information Assurance Education and/or Information Assurance Research. This brings the number of institutions participating in this highly regarded program to 106 located in 37 States, the District of Columbia, and the Commonwealth of Puerto Rico.

NSA and DHS collaborate daily, cooperating on investigations and forensic analysis of cyber incidents and malicious software, and together we look for and mitigate the vulnerabilities in various technologies that would render them susceptible to similar attacks. We each bring to these efforts complementary experience, insight, and expertise based on the different problem sets and user communities on which we concentrate, and we each then carry back to those communities the dividends of our combined wisdom and resources.

Key to the Nation's cybersecurity efforts is a public-private partnership which has been actively embraced by the Federal Government, industry, and academia. This trusting relationship includes and is based upon the common goal of improving cybersecurity, the sharing of information, and collaborative research development and innovation. A recent example of this collaboration is last month's fifth annual Security Automation Conference at the Baltimore Convention Center, co-hosted by NSA, NIST, DHS, and the Defense Information Systems Agency. This conference brought together nearly 1,000 representatives from the public and private sectors and demonstrated the benefits of automation and standardization of vulnerability management, security management, and security compliance.

As Lieutenant General Alexander, NSA's Director, stated clearly in his address to the RSA Security Conference this past April, Cybersecurity is a big job, and it is going to take a team to do it. We will bring our technical expertise, and working with many others in the public and private sector, we will comprise the team the Nation needs to address this challenge.

This concludes my remarks. I would be pleased to answer any questions from you and other members of the Subcommittee.

[The prepared statement of Mr. Schaeffer appears as a submission for the record.]

Chairman CARDIN. Again, thank you for your testimony.

Mr. Chabinsky.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00013 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

STATEMENT OF STEVEN R. CHABINSKY, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. CHABINSKY. Good morning, Chairman Cardin, Ranking Member Kyl, members of the Committee and Subcommittee.

The FBI considers the cyber threat against our Nation to be one of the greatest concerns of the 21st century. The most sophisticated of our adversaries, which includes a number of nation states and likely some organized crime groups, have the ability to alter our hardware and software along the global supply chain, to conduct remote intrusions into our networks, to establish the physical and technical presence necessary to reroute and monitor our wireless communications, and position employees within our private sector and Government organizations as insider threats awaiting further instruction.

The FBI has not yet seen a high level of end-to-end cyber sophistication within terrorist organizations. Still, the FBI is aware of and investigating individuals who are affiliated with or sympathetic to al Qaeda who have recognized and discussed the vulnerabilities of the United States infrastructure to cyber attack, who have demonstrated an interest in elevating their computer hacking skills, and who are seeking more sophisticated capabilities from outside of their close-knit circles.

To meet these challenges, today's FBI has the largest cadre of cyber trained law enforcement officers in the United States, numbering over 2,000. Internationally, the FBI operates 75 legal attaché offices and sub-offices around the world.

To be sure, while protecting the United States against cyber-based attacks is one of the FBI's highest priorities, we are always mindful that doing so must be achieved while safeguarding civil liberties and privacy rights. In that regard, the FBI complies with the Attorney General guidelines for FBI domestic investigations and receives invaluable support from the Department of Justice's Computer Crime and Intellectual Property Section, the Department's National Security Division, and U.S. Attorney's Offices throughout the country.

Although an unclassified forum is not suitable for discussing the FBI's counterterrorism and counterintelligence cyber efforts, our investigative success on the criminal side provides a glimpse into our capabilities and strategic partnerships that can be used against any adversary. For today, let me focus on the FBI's strong leadership and expertise in investigating financial cyber crime.

You may have read last year about the transnational organization that used sophisticated hacking techniques to withdraw over $9 million from 2,100 ATM machines located in 280 cities around the world, all in under 12 hours. I would not be surprised if Hollywood makes this one into a movie. From my perspective, the best part is the ending. Based on a successful FBI-led investigation with especially strong support from the reporting victim and Estonian law enforcement, just last week a Federal grand jury returned a 16-count indictment against key members of the group, and arrests already have been made internationally.

Only a few weeks earlier, the FBI's Operation Phish Phry brought down a transnational crime ring that engaged in computer

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00014 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

intrusions, identity theft, and money laundering. The case resulted in a 51-count Federal indictment, charging 53 U.S. citizens, while FBI in coordination with Egyptian law enforcement identified 47 Egyptian suspects directly involved in the criminal conspiracy. This year, the FBI and the Financial Services Information Sharing and Analysis Center, the FS–ISAC, also forged a best practice for Government-private sector information sharing. We co-authored an advisory based on ongoing FBI investigations that were then distributed to the 4,100 members of the FS–ISAC, over 40 of which are themselves associations, and shared with bank customers to prevent further victimization.

At the consumer level, the FBI established and leads the Internet Crime Complaint Center in partnership with the National White Collar Crime Center. www.ic3.gov is the leading cyber crime incident-reporting portal, having received over a quarter of a million complaints just last year.

We are also proud of the FBI's cooperative efforts with the United States Secret Service. In order to support the Secret Service's cyber crime authorities, the FBI provided the Secret Service with over 1,800 cyber intelligence reports and analytic products in fiscal year 2009 alone. The Secret Service also is a full-time member of the FBI's National Cyber Investigative Joint Task Force, and the FBI has invited the Secret Service to partner with us at the Internet Crime Complaint Center and the National Cyber Forensics and Training Alliance. Operationally, we are providing the Secret Service with the opportunity to participate in FBI-led investigations, which most recently provided the Secret Service with information relevant to their successful investigations of intrusions into Heartland Payment Systems and TJX Companies.

Each of the above examples demonstrates that taking advantage of all of our country's skills and knowledge, leveraging our Nation's resolve and common cause, provides significant advantages that are leading to increased and repeatable successes.

In conclusion, I am grateful to the Subcommittee for this chance to highlight the FBI's strengths in combating cyber terror, cyber espionage, and cyber crime in a manner that protects privacy rights and civil liberties, and to recognize the partnerships that allow us to meet this ever growing economic and national security problem.

In that regard, I would also like to particularly thank the members of this panel with whom the FBI partners every day.

I am happy to answer any questions you may have. Thank you.

[The prepared statement of Mr. Chabinsky appears as a submission for the record.]

Chairman CARDIN. Let me thank all of our witnesses from the Department of Justice, from Homeland Security, NSA, and from the FBI. I do not know if we feel any better after listening to your testimony, but I think we understand the risk, and the risk is that we can have spies, soldiers, and criminals anyplace in this country placed overnight, and, Mr. Reitinger, you mentioned that we need to be more aware. But I am not so sure we know when, in fact, we have been invaded. Certainly that is true with the less sophisticated users who do not have the same type of security systems that perhaps the Government has. But it is unclear that we really even know when we have been attacked. And it is very possible today

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00015 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

that major information systems have been compromised, and we are not clear whether there is an operational plan to use that at this point or not.

Which brings me, I guess, to the risk factors. We are concerned that other governments are, in fact, actively involved in trying to compromise our cybersecurity. We know that terrorists are interested in invading us. We know that criminals have game plans to try to advance their particular causes. And then you have the lone-wolf hackers who just want, for whatever reasons, to compromise cyberspace.

Is there a common strategy here that we can use to protect us against other countries, against terrorists, against criminals, against hackers? What is the common strategy that the United States needs to employ in order to make us less vulnerable to these types of attacks? Who wants to start?

Mr. Reitinger.

Mr. REITINGER. I will start with that, sir, and then look for additional contributions from the other people on the panel.

There is a common strategy, but it is not a one-prong strategy. As a number of us said, there is no silver bullet here, sir. In some cases, there will be different strategies. For example, one might use different strategies with regard to single hackers or organized criminal groups as opposed to terrorists or nation states. But broadly across all of them, we do need to up our defensive game, and that is essentially our role in the Department of Homeland Security, at least the components that report up to me.

We need to make sure that we are, as you suggested, raising awareness across the spectrum.

Chairman CARDIN. How do you raise awareness when you do not know, in fact, that you have been compromised or that there is something in your software or hardware that can be used against you? As I understand it, the technology is not at that point where particularly in the private sector they do not know whether their software program has been compromised, as I understand it.

Mr. REITINGER. Sir, it gets complicated, but I think there are three responses to that. The first is that, obviously, supply chain attacks are of concern, and we are not where we need to be as a Nation yet in terms of ability to prevent and deter supply chain attacks. It can be very difficult to determine if software has vulnerabilities or does not, and that is both—we need to work on practices and procedures in that regard and on technology.

With regard to end users knowing whether they have been compromised or not, I think there are a couple of pieces. The first is that we need to make sure that they know about the threat and they are at least aware of the simple things that they can do to protect themselves. That was actually the message, one of the key messages of Cybersecurity Awareness Month, to make sure that we were trying to communicate as broadly as possible that there are very simple things that end users can do to cutoff broad avenues of attack—you know, keep their software up to date, run antivirus, some fairly simple steps.

With regard to knowing whether they have been compromised or not, we have provided tips to end users, things they should watch for that might indicate, for example, that their computer had been

compromised as a botnet. But there is a broad technology agenda there, too, sir. It remains the case that it is too hard for individual users and even small and medium businesses to secure their systems. We need to as a Nation and as an IT ecosystem continue to make it more simple for people to institute protections, to determine if they have been compromised, and to make sure they stay secure.

Chairman CARDIN. Mr. Chabinsky, you said the good news is that we brought indictments against those who robbed us. The bad news is they were able to rob us, they were able to get money. And every day, as I understand it, there is money being stolen through cyberspace.

So there is clearly a vulnerability here. Clearly, we want to bring criminal charges to those who violate our criminal statutes. But I think our first objective is to prevent this from happening.

Mr. CHABINSKY. Yes, Senator. The case that you are referring to actually has an interesting component that I did not mention in my oral testimony in which, while we were investigating that case, we received information from our foreign law enforcement partners that showed a targeting list of other banks that were going to become victims. And we were able actually to notify each of those banks. We actually went in person with FBI agents to notify each bank so that they would be prepared and they were able to prevent further crime. So in that example, the bad news part of the story, Senator, as you mentioned, is that we already had victims. The good news part is we were able within that case to prevent further victimhood.

The same would go for our relationship with the Financial Services ISAC in which, by seeing a growing trend which amounted to 200 cases, that is the bad news part of the story. There were 200 cases that we had in which we saw victims.

Nationwide, we probably prevented thousands more by getting the information out to each of the banks and for them to then provide with their customers to show them how they could avoid future schemes.

The FBI is trying to have better preventive efforts by undercover operations, by way of example, so that we could penetrate some of the organizations that are planning attacks and in that way know their intent before they have the ability to act upon it. But it is a difficult problem, sir.

Chairman CARDIN. Mr. Schaeffer, first of all, I have been to NSA many times, and I am always impressed by the quality of work that is done there. I think our first line of attack is to try to get the right intelligence information and develop the technologies in order to counter what those who want to attack us want to do. At NSA, you are very much involved in both of those areas, although your intelligence collection, of course, is international.

How do you stay ahead of the curve? It seems to me normally you would want to get experienced people on staff that are expert in this area, but in cyber issues it seems like the young people—it is more people coming out of college developing new technologies. How do you stay ahead of the curve here?

Mr. SCHAEFFER. Well, sir, we do exactly what you said. We recruit, we hire, we train those bright young minds that are coming

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00017 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

out of the colleges and universities today. I started at NSA as an engineer, and I am certainly glad I am not competing with the intellect and the capabilities that are coming out of the colleges and universities today. They have got tremendous capabilities.

So we take experienced personnel who are deeply steeped in vulnerability discovery and understanding how systems break and how they can be broken, and use the technology knowledge that the young workforce brings into our environment, and it is a collaboration. It is a mentorship. It is a partnering between more experienced employees and the younger folks who do bring the latest technology knowledge into the space.

We, of course, have a research organization that tries to stay ahead, helping us understand what breakthrough technologies or what significant technologies that may be coming down the road at a later point in time, that we need to be prepared to help understand how to protect and defense those technologies in the information space.

So it is a combination. It is bright young people coming into the organization. It is experienced people. It is great tools and technology that the Nation gives us to help work this problem.

Chairman CARDIN. And we would invite you to share with us if there are additional tools you need in regards to this issue. We understand the politics of OMB and all the other areas that you have to deal with. But I think we want to hear independently from you as to what tools are necessary for you to be able to effectively deal with this threat against our country. So we would appreciate that.

And for Mr. Baker, you also indicated that there may be needs for changes in our law as it relates to the ability to properly protect this country, but also protect the civil liberties of the people who live in America. And we would invite you to be open in that process working with us to help develop the legal framework that you need. We know what we went through with FISA. We know what we went through on some of the issues. We want to work collectively here. We do not want to work in an adversarial role as to what is necessary to give you the tools you need, but also to protect the civil liberties of people in this country.

Mr. BAKER. Yes, Senator. Thank you very much. We recognize that, and we appreciate the opportunity to work with you on these very complex and important issues.

Chairman CARDIN. Thank you.

Senator Kyl.

Senator KYL. Well, let me begin by reiterating the point that the Chairman just made. These hearings give us the opportunity to hear some things from you, but we just get a sketch. We just touch the surface. And we are also looking for what we can do to help, both in terms of resources that might be available or needed or legislative authority. And so that invitation really is extended to each of you and the others with whom you work.

And I think the Chairman put his finger on it by inquiring about a common strategy. Let me see if I can bore down into that just a little bit. And I do not want to get into organizational charts because they make my head spin, but to try to understand just in a very basic way how our Government—who is in charge, if anyone is, and how we structure the mechanisms that can be useful to pro-

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00018 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

tect across broad spectrums of society, including Government agencies, contractors, private businesses, utilities, and universities and others that are all subject to the same kinds of attacks and, therefore, about which some commonality would seem to be in order.

And maybe, Mr. Schaeffer, let me begin by asking you since, as I understand it, NSA has been given some kind of overall lead in this, but I am not sure that the authority is nailed down. And I know that there are some conflicting views as to who all should have what authority and whether there should be somebody in charge. Maybe you could give us your understanding, and then I invite each of the rest of you to comment on that as well.

Mr. SCHAEFFER. Well, sir, I think I would first point to the comment that General Alexander made back at the RSA Conference, and that is, this is a team sport. You are absolutely correct, there are various authorities that exist in departments and agencies across the Government. Within NSA, our responsibility for national security systems is just a portion of the overall set of networks. We work collaboratively with the Department of Homeland Security, the National Institute of Standards and Technology, and others to help other elements of the Government.

I think the great benefit is that what we do for U.S. Government systems, whether that is in the development of configuration information, whether it is standards, all that is directly extensible into the private sector. The kinds of policies and procedures that we outline for U.S. Government systems can, in fact, be adopted by critical infrastructure elements and others across the community. We think in terms of the things that we can do to protect the network environment, individuals can adopt those mechanisms as well.

I cannot underscore enough a comment that Mr. Reitinger made about just the basics. How do you harden systems? It is good configuration management. It is good patch management. It is good access control. All the kinds of principles and practices that we as individuals and we as organizations need to put in place such that the policies that exist, disparate and varied though they are, can, in fact, have an effect on the overall assurance of the operating environment in which we conduct our business today, whether that is warfighting, whether that is Government, or otherwise.

Senator KYL. Let me just bore down a bit. Mr. Reitinger, let me put that question to you, because I gather that there is some connection between the Government on the one hand and all of the private sector on the other hand, through Homeland Security, but I am not exactly sure. I do not know if what I said is correct or not. But if anybody does it, I presume you would. How do those mechanisms that you appreciate the need for, because you are at the highest level of development, get translated down into all the different sectors of our society where they are really needed?

Mr. REITINGER. Absolutely, sir. As Mr. Schaeffer indicated, this is a team sport, but it is not even football or baseball, if I could perhaps unduly extend the analogy. It is more like soccer. We are all playing positions, and we need to execute in our individual roles. This is going to remain a horizontal activity across Government.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00019 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

One of the roles that we have in the Department of Homeland Security is serving as the bridge into the private sector, sort of the broader dot-com and the infrastructures that are out there that we need to protect. So we built a structure, the National Infrastructure Protection Plan, and a set of sector coordinating councils that bring people from all of those different sectors together to collaborate with Government.

There is also an additional structure next to that that works specifically on operational issues, the set of information-sharing and analysis centers that work both through that structure and with the United States CERT, but also more particularly with their sector-specific agencies. So, for example, Mr. Chabinsky talked about the Financial Services ISAC. That is an operational body working clearly in the financial services sector that would partner with US–CERT on some of the defensive measures, on some law enforcement material, and some of the work coming out of the Bureau's infrastructure protection capabilities would partner with the Bureau.

So we have built a structure where there are multiple ways to work together, and we are continuing as a Government and more broadly in the private sector to refine the roles and responsibilities we have all got.

So, for example, one of the outcomes of the Cyberspace Policy Review is that we need, in the event of a significant incident, to be able to respond as one Nation. So there is an effort going forward called the National Cyber Instant Response Plan to devise a highly actionable set of policies and procedures that will enable all of the different Government agencies to work effectively with the private sector in the event of a significant incident. And we are driving toward having a draft ready at the end of this year or the start of next year that we are actually going to test at the start of next year and that will even more affirmatively exercise in the Cyber Storm III exercise that will take place in September of next year.

Senator KYL. Great. I have just another minute or so. Would either of the two of the Department of Justice and the FBI witnesses like to comment as well, please?

Mr. BAKER. Well, just briefly, Senator. Thank you.

I guess in response to your question about who is in charge, from the executive branch it is the President who is in charge, and there is a very active effort run out of the White House. We meet weekly. There is a big group that meets weekly or almost weekly. There are sub-groups that meet continually on a variety of different topics.

Senator KYL. Excuse me, but who convenes that meeting or nominally sets the agenda?

Mr. BAKER. It is the National Security Council, a director-level person, I believe, in there who is running those meetings. And so there is a very active—I made a brief reference to it in my opening remarks—a very active policy, operational, technology review that is going on continually to try to address some of these very, very difficult legal, technical questions that we are facing.

Chairman CARDIN. Would the Senator yield just for one moment?

Senator KYL. Sure.

Chairman CARDIN. Is that structure by just de facto or has the President requested this, the National Security Council coordinating this activity? Or is it just taken up because of its——

Mr. BAKER. The accurate answer is I do not know the exact origin of that, Senator. We can find that out and get back to you. But it is very structured, so it is not just de facto, it has not just emerged on the back of an envelope.

Chairman CARDIN. We would appreciate that. Thanks.

[The information referred to appears as a submission for the record.]

Senator KYL. Mr. Chabinsky, anything you want to add to that?

Mr. CHABINSKY. I would like to support and add a little bit more to Mr. Baker's comments. The National Security Council has been working through the Interagency Policy Committee to coordinate the cyber security. The President immediately upon entering office asked for a Cybersecurity Policy Review. After that review was completed, the President adopted the Comprehensive National Cybersecurity Initiative and provided additional short-, mid-, and long-term recommendations for moving the community forward. And the community has stayed on top of that through the leadership of the Office of the Director of National Intelligence. The Joint Interagency Cyber Task Force continues to monitor and coordinate the 12 interdependent initiatives within the Comprehensive National Cybersecurity Initiative working with each of the agencies on performance measures and letting the President know on a quarterly basis how the community has organized to respond.

Part of that Comprehensive National Cybersecurity Initiative involves very strong partnership with the private sector and academia, led by the Department of Homeland Security.

In addition, part of that partnership includes gathering the intelligence agencies, law enforcement agencies, homeland security agencies in common cause both for shared situational awareness, as provided by the National Cybersecurity Center which Mr. Reitinger directs, and US-CERT at the Department of Homeland Security, and the FBI takes a leadership role for domestic investigative coordination at the National Cyber Investigative Joint Task Force.

For its part, the FBI has additional partnerships not only with the critical infrastructures, but within its InfraGard Program that started in 1996. We have expanded that program to include over 33,000 members of the private sector located throughout 87 cities in the country. In fact, InfraGard now has all but eclipsed the size of the Federal Bureau of Investigation showing that partnerships are both required and looked for by industry. So that has been enormously successful, as have our partnerships with the National Cyber Forensics and Training Alliance and the National White Collar Crime Center.

So we are working together, and I think that there is more occurring than what might otherwise meet the eye, and we are moving forward in collaboration both as a Government and with the private sector and industry, and with our international partners.

Senator KYL. Thank you.

Chairman CARDIN. Senator Kaufman.

Senator KAUFMAN. Thank you, Mr. Chairman.

I would like to follow up on Chairman Cardin's question. He said, if you do not know you are under attack, how do you proceed? I would just like to talk a little bit, Mr. Reitinger—and others can

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00021 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

chime in—about when you are under attack. I was involved with an agency of the Federal Government that was under a massive attack. They knew they were under attack, and the consultants told them afterwards not to publicize it because they were pretty sure it was a hacker and that the hacker was looking for attention.

Now, when you are in a situation when you do not know whether it is a hacker, you do not know if it is a foreign government, you do not know if it is a terrorist, you do not know if it is a criminal, how do you proceed to deal with a cyber attack that you have already taken?

Mr. REITINGER. Generally, the defensive measures that you would use would depend less on the source of the attacker and more on what the attack looked like and how you would defend against it. So there might be a set of defensive protections you would use for a denial-of-service attack, a separate set for intrusions, and a separate set for something like an Internet fraud activity.

So in all of those cases, we in the Department of Homeland Security, the United States Computer Emergency Readiness Team or Cyber Emergency Readiness Team, would be responsible for working with the department or agency to help them defend their networks and to respond to the attack. We in DHS worry less about attribution and more about defense.

In terms of responding to the attack and attribution, that sort of activity would be pursued by an entity like the Secret Service or the Federal Bureau of Investigation, and so that would be an area within their area of responsibility, and either we or the Department or the affected department or agency would work effectively with them.

Senator KAUFMAN. And under no circumstance will you publicize the attack or let the public know that there had been an attack on the agency?

Mr. REITINGER. That is not generally our role. That would be the department or agency's role. In point of fact, there are often reasons not to publicize attacks because it could interfere with an ongoing criminal investigation.

Senator KAUFMAN. And then if you were an agency, just a general agency out there, to kind of follow up on Senator Kyl's comment, who would be there to advise you how to proceed?

Mr. REITINGER. Lots of people could be there to provide advice to you on how to proceed. US-CERT could provide and would provide advice as part of its overall responsibility to help coordinate the security of civilian Government agencies. And with regard to law enforcement activity, the FBI or the Secret Service, depending upon the particular type of activity, could provide advice. So depending upon what had happened different, people could provide advice.

In addition, advice from the private sector can be available directly to the agency because they will have partnerships and vendors that they work with, and advice from the private sector is also available through US-CERT and the different partnerships that both DHS has created and the sector-specific agencies have created in each of the different critical infrastructure sectors.

Senator KAUFMAN. Mr. Schaeffer, in your testimony you talked about publicizing and the meetings you had and the forums and the rest of it. Is there conflict between publicizing how people should proceed in order to be prepared for cybersecurity and the fact that when you do that, you kind of let the bad guys know exactly what you are doing in order to stop them?

Mr. SCHAEFFER. Well, sir, I think the challenge is how do we get everyone up to a certain level of assurance. There is a lot that we can state publicly, it is unclassified, a lot that we can do to help individuals and system owners harden the network environment in which they operate. That is good. That is common sense. That is good network hygiene. There are common principles that people ought to be using anyway that are quite public. And so it does not disclose anything that would help an adversary know how to attack a system or intrude upon a system. It actually makes that job harder for the individual, raising the ante somewhat, causing them to have to resort to more sophisticated means to gain entry into a system.

So the harder we can make the general network environment, the easier it is going to be to detect when, in fact, something does go wrong, a system has been intruded upon.

Senator KAUFMAN. You said in your testimony, you talked about the use of proper operating system configurations to help. What portion of the problem could be solved if people used proper operating system configurations, do you think?

Mr. SCHAEFFER. Well, that is a wonderful question. We believe that if one institutes best practices, proper configurations, good network monitoring, a system ought to be able to withstand about 80 percent of the commonly known attacks, mechanisms against systems today. But you can actually harden your network environment to raise the bar such that the adversary has to resort to much, much more sophisticated means, thereby raising the risk of detection and so forth.

Just an example. We are much more in sync now with the release of new technology. It was just a couple of weeks ago that Microsoft released Windows 7. We have had a longstanding relationship in working with Microsoft to help improve the security of that operating system, and it was almost coincident with the release of Windows 7 that Microsoft also released the Security Configuration Guide, thereby enabling users to, out of the box, activate about 1,500 security settings that otherwise would be turned off.

And so there is a tremendous amount of capability that is enabled through configuring software applications more effectively from a security standpoint. Of course, then they have to be maintained, and that is the kind of constant vigilance that goes along with maintaining a good security posture.

Senator KAUFMAN. OK. Just one short question, Mr. Reitinger. Is there anybody in your Department involved with the security of electronic voting machines?

Mr. REITINGER. I believe we have had some involvement, but I need to get back to you.

Senator KAUFMAN. Could you get back to me on that?

Mr. REITINGER. Yes.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00023 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

[The information referred to appears as a submission for the record.]

Senator KAUFMAN. Thank you very much.

Thank you, Mr. Chairman.

Chairman CARDIN. I would just comment, 80 percent against an attack on our country would be, I think, unacceptable. But I understand the challenges that we are facing, but leaving a 20-percent risk factor is still a high risk factor.

Senator KAUFMAN. I wonder what it is right now.

Chairman CARDIN. I am sure it is much higher.

Senator KAUFMAN. The point is if we get to 80 percent they have to expose themselves more. It is not just that it is 80 percent—obviously, we want to be 100 percent. But if they are 80 percent, what you are basically saying, Mr. Schaeffer, if I am right, is that in order to pierce a wall that is 80 percent, they have to expose themselves more, and it makes it easier to catch them. So that 80 percent is more than just like our normal getting 80 out of 100. It presents them with a bigger problem, and then they have to show more what they are about in order to——

Chairman CARDIN. I think that is a very good point. I guess my point is that we would never prepare a defense budget based upon an 80-percent effectiveness. So it is——

Senator KAUFMAN. I totally agree with you. I totally agree with that.

Chairman CARDIN. Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman Cardin.

Are all of you or any of you satisfied with the existing legal structure within which you are presently operating?

Mr. BAKER. Senator, that is complicated question. I think the answer to it is no.

Senator WHITEHOUSE. Does anybody disagree? Are there any yeses on the panel?

[No response.]

Senator WHITEHOUSE. OK. Nobody is satisfied. That said, can we expect administration legislative proposals at some point?

Mr. BAKER. As I mentioned in my opening remarks, we are very eager to work with Congress——

Senator WHITEHOUSE. Being eager to work with us and having a proposal are two different things.

Mr. BAKER. We do not have a proposal today. We are definitely debating these kinds of issues inside the administration. But as I mentioned in my opening remarks——

Senator WHITEHOUSE. With a view——

Mr. BAKER. I beg your pardon?

Senator WHITEHOUSE. With a view toward preparing proposals?

Mr. BAKER. With a view to deciding whether we should propose changes and, if so, how, because we do not want to mess up, to put it bluntly, the existing authorities that we have that provide a huge amount of capability to collect both law enforcement information and foreign intelligence information and, importantly, protect civil liberties and privacy. So we do not want to make mistakes because this area is so complicated, as you know from your debates about the FISA amendments that the Chairman referenced earlier that is a very complicated area. This area is equally as com-

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00024 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

plicated. There are many statutes you have to consider, and not only Federal statutes but also you have to consider State law, foreign law, and international law, because these are things that impact this area as well with respect to the private sector in particular.

So it is a complicated area, and we are very cognizant of the need to review these authorities closely and make sure that we are doing the best that we can today.

Senator WHITEHOUSE. By what process will that analysis be undertaken?

Mr. BAKER. Well, there is this interagency process that I mentioned before with all of the different agencies that have equities in this area, and it will proceed, I believe, in the normal—you know, once proposals are developed, it will proceed in the normal interagency process. Everybody gets a chance to look at what the proposals are and make sure that we are not doing anything one way or the other that is not effective or will not be effective.

Senator WHITEHOUSE. But the original development of those proposals would be through the interagency process led by the National Security Council that you have looked at?

Mr. BAKER. I think that is fair to say, Senator, yes. DOJ plays an active role in that process. We have got all the different—I mean, every one of these agencies has a General Counsel's office that are reviewing these things. So I think that is fair to say, yes.

Senator WHITEHOUSE. Would you be the lead agency for that effort?

Mr. BAKER. DOJ is always the lead agency when it comes to—we obviously play a key role in reviewing the legal authorities with the legal advisers from the National Security Council, Homeland Security Council, all the different General Counsel's offices representing the agencies that are here today, plus more.

Senator WHITEHOUSE. Everybody else agreed? I think your microphone may not be on.

Mr. REITINGER. Sorry. It seems to be a problem I have got today. As Mr. Baker indicated, the Cyberspace Policy Review, the work that led to that, identified a number of legal issues, and those are all under examination, including the various authorities that agencies have and whether or not we—whether the administration would want to propose things. I believe the process would be essentially as he says, with agencies looking at their own needs and working through the interagency process to propose things, if called for, to Congress.

Senator WHITEHOUSE. On a separate aspect of this topic, the problem of attribution is one that I think every witness has mentioned during the course of this hearing, which, of course, on the flip side is the problem of deniability by the sponsor of the attack, which inhibits deterrence as a countermeasure by our country.

However, even where attribution through the maze of servers and electronic connections out there cannot be specifically established, the fact that a fighter plane's systems have been hacked and are particularly useful to one particular country or that very significant code developed by the American private sector appears verbatim in the code of competitors in another country and you can sort of connect the dots at that point. And it is a little bit beyond

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00025 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

a pure law enforcement matter because you may not be able to actually prove all the way through, and if it is a Government act, it is a little hard to get the Government in a court of law.

What are you all doing to—what is being done to build a foundation for diplomatic dialogue with the nations that are most responsible for the massive, persistent, and aggressive waves of cyber attack that we are experiencing in a more general way? There is a point where you can say, "Look, OK, you are not doing it. Sure. If it continues to happen, here are the consequences." That is something that can really only be done at a diplomatic nation-to-nation level. I know the President is in China now. Where are we in terms of trying to push back diplomatically against foreign sovereign-sponsored cyber attack?

Mr. REITINGER. Let me briefly answer that question, sir, and then turn to the question of attribution, if I might, because you raised a number of points there that I think it would be important to touch on.

One of the action items coming out of the Cyberspace Policy Review, another one of them, was specifically to develop more focus on what the right international framework is here, and, clearly, we need both closer relationships with allies and overall an approach to how we are going to have a secure global ecosystem going forward. So that is an area of focus, and work is going on interagency right now about the right international approach.

The other thing, I wanted to turn briefly to attribution, because you talked a little bit about that at the start. Obviously, actually attributing conduct is not clearly a role of the entities that report up to me, like the United States Cyber Emergency Readiness Team, US–CERT. That is more a role for, for example, the Department of Justice and the FBI.

But there is another side to attribution which I think does go to what you are talking about, sort of the positive attribution, not where you want to say, "I have been attacked. Who did it?" but, "I only want to let in people into my systems when they have proven who they are." So that is more about authorization and authentication.

Another action item coming out of the policy review—and if you talk about broadly cutting out avenues of attack, there is little that we could do that would be more effective than enabling broad, voluntary, interoperable authentication with privacy protections built in at the start so it is much easier to defend your systems and your perimeter and only let in the people, the software, or the devices that you want to.

Senator WHITEHOUSE. My time has expired. Thank you, Chairman.

Chairman CARDIN. Thank you.

Just following up on Senator Whitehouse's point on the protection of privacy in our current laws, there has been the implementation of the EINSTEIN I, II, and now III, which is being used by our agencies to protect against cyber attacks. As I understand it, it has the capacity of obtaining personal information from innocent Americans. And I guess my question to you, Mr. Baker, is: Are you satisfied that the current implementation of these countermeasures is consistent with our privacy laws and that minimization is being

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00026 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

used to prevent the dissemination of information that is otherwise protected?

Mr. BAKER. Thank you, Senator. As the Committee knows, we have done an extensive legal analysis of the EINSTEIN II initiative and made available the OLC opinions regarding—two OLC opinions regarding that matter which are publicly available on OLC's website. So our analysis of that program is that it does comply with the Fourth Amendment and with the various statutory requirements. It meets the various statutory requirements that are out there.

In terms of minimization and use of the information and so on, I mean, there are procedures in place, as reflected, I think, in the Department of Homeland Security's privacy impact statement or assessment with respect to EINSTEIN II, that describe the kinds of procedures and policies that they implement to ensure that information regarding—personally identifiable information or other information generated from that program are handled appropriately. And so I believe that we are satisfied with that to date.

Chairman CARDIN. And EINSTEIN III, as I understand it, is now in the process of being developed and implemented?

Mr. BAKER. I will defer to Mr. Reitinger on the description of EINSTEIN III, but——

Chairman CARDIN. The Department of Justice has not had any impact on III?

Mr. BAKER. The Department of Justice has conducted a legal analysis of EINSTEIN III. I am not able to describe that or discuss that in this setting today, but we have conducted such an analysis and, I believe, made that available to committees of the Congress.

Chairman CARDIN. Mr. Reitinger.

Mr. REITINGER. Thank you, Mr. Chairman. Obviously, EINSTEIN I and EINSTEIN II are in deployment. EINSTEIN III is still in development. We are working closely with our partners in Government, including the Department of Justice, on what that ought to look like and how we can best protect privacy. I can spend more time describing the protections for privacy in EINSTEIN II. Mr. Baker touched on them, but they are fairly broad. They include policy and procedure. As our Privacy Impact Assessment described, how we collect information, when we retain and how we retain information, and how it is disclosed.

It includes training. We provide training to those responsible in US–CERT for operating the EINSTEIN system. There are three levels of training in the Department of Homeland Security: general privacy training, specific training for those who conduct the EINSTEIN system, and going forward, there will be specific training on EINSTEIN III.

Oversight mechanisms, both the Office of Privacy and the Office of Civil Rights and Civil Liberties and other components of the Department of Homeland Security can provide oversight into the mechanisms that are used. And, in addition, within the Office of Cybersecurity and Communications, there is an identified compliance and oversight officer whose job it is to ensure compliance with the rules.

And, last, there is transparency. I think we have received some praise for the fact that we have gone forward and been forward

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00027 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

leaning with our Privacy Impact Assessments for EINSTEIN I and II, and it is our intention to be as transparent as possible consistent with the need for secrecy in some areas.

Chairman CARDIN. Let me go back to Senator Whitehouse again. On EINSTEIN III, the Department of Justice, is that one of your concerns about the current legal structure being adequate? Or are you able to work through EINSTEIN III within the current legal framework?

Mr. BAKER. I think, Senator, I am not able to describe the legal analysis with respect to EINSTEIN III in detail today, but what I will just—I will say that, as I describe, there is a range of statutes—the Fourth Amendment, obviously, and then the range of statutes that apply in this area. So anytime you are doing anything with electronic communications, storage, transit, however it—I am not speaking about EINSTEIN III in particular, but any type of program, you have to go through a whole range of different issues that you have to analyze. So it is complex in that sense. The statutes are complex. The legal regime is complex. And, therefore, the analysis is complex.

If I could just amend my comments from before, with respect to EINSTEIN II, there are still discussions that are going on with respect to the procedures of handling some of the data, in particular data that comes into the Department of Justice, for example, from a variety of different sources. So not all of the privacy issues with respect to EINSTEIN II have been resolved. There is still work going on in that regard, so I just wanted to note that.

Chairman CARDIN. And just following up on Senator Whitehouse, this Committee is very interested in understanding the legal challenges, both in obtaining the information you need and protecting the privacies. And if this is not the right forum to talk about it, we invite an opportunity to review it.

Now, Senator Whitehouse also serves on the Intelligence Committee, so he is in a position where he can obtain information both through the Intelligence Committee and the Judiciary Committee.

Senator WHITEHOUSE. Usually a day or so after the New York Times gets it.

[Laughter.]

Chairman CARDIN. Senator Kyl.

[Pause.]

Chairman CARDIN. If our colleagues are agreeable, we are going to dismiss this panel and go to the second panel because we are told it is likely to be votes starting soon. Thank you all very much for your testimony.

Chairman CARDIN. Our second panel consists of Gregory Nojeim, who is the senior counsel at the Center for Democracy & Technology and the director of its project on freedom, security, and technology. In this capacity, he conducts much of CDT's work in the area of national security, terrorism, and Fourth Amendment protections. He is also co-chair of the Coordinating Committee on the National Security and Civil Liberties of the Individual Rights and Responsibilities Section of the American Bar Association.

Larry Clinton is president and CEO of the Internet Security Alliance. He is a member of the experts panel created by the General Accounting Office at the request of the House Committee on Home-

land Security to assess and make recommendations to the Obama administration on cybersecurity.

Larry Wortzel is Vice Chairman of the U.S.-China Economic and Security Review Commission. He is a retired Army colonel who served two tours of duty as a military attache in China. For 25 years of his 32-year military career, Dr. Wortzel was an intelligence officer.

If you all would please rise so I can swear you in. Do you affirm that the testimony you are about to give before the Committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Mr. NOJEIM. I do.

Mr. CLINTON. I do.

Mr. WORTZEL. I do.

Chairman CARDIN. Thank you all very much. Without objection, your entire statements will be made a part of the Committee record. You may proceed as you see fit, starting with Mr. Nojeim.

STATEMENT OF GREGORY T. NOJEIM, SENIOR COUNSEL AND DIRECTOR, PROJECT ON FREEDOM, SECURITY & TECHNOLOGY, CENTER FOR DEMOCRACY & TECHNOLOGY, WASHINGTON, DC

Mr. NOJEIM. Thank you, Chairman Cardin, Ranking Member Kyl, members of the Subcommittee. Thanks for the opportunity to testify about cybersecurity and civil liberties on behalf of the Center for Democracy & Technology. CDT is a nonprofit, non-partisan organization dedicated to keeping the Internet open, innovative, and free.

The United States faces significant cybersecurity threats. Computer hackers have penetrated Government systems and have stolen massive amounts of sensitive information. They have penetrated financial networks and have stolen millions of dollars. While the need to act is clear, it is essential that we take a nuanced and incremental approach. We ask that you keep a key distinction in mind as you go forward. Policy toward Government systems can be much more prescriptive than policy toward private systems.

The characteristics that have made the Internet successful—openness, decentralization, user control—they may be put at risk if heavy-handed cybersecurity mandates are applied to all critical infrastructure.

When he unveiled the White House Cyberspace Policy Review on May 29, President Obama correctly emphasized that the pursuit of cybersecurity must not include governmental monitoring of private networks. Monitoring these systems is the job of private sector communications providers. They already do it today pursuant to self-defense provisions in current law. The Wiretap Act allows communications providers to intercept, use, and disclose—to both their peers and to the Government—communications passing over their networks while they are engaged in activity necessary to protect their own rights and property. ECPA provides similar authorities for disclosure of stored communications. Furthermore, the Wiretap Act allows service providers to invite in the Government to intercept the communications of computer trespassers. These provisions do not authorize ongoing or routine disclosure of traffic by the pri-

vate sector to the Government, nor should they. The Subcommittee should consider whether it is necessary to clarify these provisions and to require public statistical reporting on their use.

While current law authorizes providers to make disclosures to protect themselves, what about disclosures to protect others? There might be a need for a very narrow exception to the Wiretap Act and to ECPA to permit providers to make voluntary disclosures about specific attacks and malicious code to protect other providers. We urge the Subcommittee to approach this issue very cautiously, for exceptions intended to promote information sharing could end up harming privacy.

While the private sector protects its systems, the Federal Government clearly has responsibility to monitor and protect its own systems. Caution and transparency are both required to avoid chilling communications that Americans have with their Government. The DHS EINSTEIN system is being deployed by Government agencies to protect Government computers against attack. CDT does not object to this in principle. However, independent audits should be required to ensure that EINSTEIN does not inadvertently access private-to-private communications. Audits could also ensure compliance with strict limits on how much information is collected, with whom it is shared, and for what purposes.

We do, however, object to the secrecy that has shrouded the EINSTEIN Program. Notwithstanding the OLC opinions and the Privacy Impact Assessment that have been released, much more needs to be known about the program. Excessive secrecy undermines public trust and communications carrier participation, both of which are essential to the success of this and other cybersecurity initiatives.

On the question of identity and authentication, some have proposed sweeping identification mandates, including even a passport for using the Internet. Identification and authentication will likely play a significant role in securing critical infrastructure. They should be applied judiciously, to specific high-value targets, and to high-risk activities and allow for multiple identification solutions.

Privacy and security cannot be viewed as a zero-sum game. Measures intended to increase communications security need not threaten privacy and, indeed, they can enhance it. CDT looks forward to working with the Subcommittee to identify and promote these win-win solutions.

Thank you.

[The prepared statement of Mr. Nojeim appears as a submission for the record.]

Chairman CARDIN. Thank you very much for your testimony.

Mr. Clinton.

STATEMENT OF LARRY CLINTON, PRESIDENT, INTERNET SECURITY ALLIANCE, ARLINGTON, VIRGINIA

Mr. CLINTON. Thank you, Mr. Chairman, Mr. Kyl, Senator Whitehouse. The Internet Security Alliance is a trade association of major business users of Internet security services, so we represent banks, defense companies, IT, telecom, traditional manufacturers, pretty much anybody who uses the Internet. ISA's mission is to integrate advanced technology with the pragmatic business

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00030 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

imperatives of the owners and operators of the system, which is primarily the private sector, and coordinate that with what we hope will be enlightened public policy to create a sustained system of cybersecurity.

In November of 2008, ISA published its policy recommendations for the 111th Congress, the social contract document, which we hope to provide that sort of overarching strategy that I think the Chairman was asking about initially. We were delighted when President Obama came out with his Cyberspace Policy Review in May of 2008 because the first thing he quoted was our social contract document, and they cited about a dozen other documents of ours in terms of their report. Naturally, the ISA supports the President's position for three reasons.

First, the administration recognizes that cybersecurity is as much an economic issue as it is a technical issue. That is, by the way, we are not reaching that 80 percent we discussed during the first panel.

Second, the administration advocates the development of market incentives to improve private sector behavior with regard to cybersecurity.

Third, the President himself said that he will not be supporting mandated cybersecurity standards for the private sector. This last point is important because, as we argue in detail in our written testimony, federally mandated cybersecurity standards not only would not work, but they will be seriously counterproductive to our National economic interests and our National security interests.

On December 3rd, we are going to be releasing a new publication detailing specific steps to move from broad principles of agreement to implementation. However, given the short amount of time I have with the Committee today, I want to focus on the one issue that I believe is most important for the Committee to appreciate if it is going to legislate in the cybersecurity space, and that is, in order for us to achieve a sustainable system, we must fundamentally change the economic equation with regard to cybersecurity.

The dispiriting realization with regard to cybersecurity economics is that all of the current incentives favor the attackers. Cyber attacks are comparatively cheap and easy to execute. The profits that can be generated from cyber attacks are enormous. Cyber defense perimeter is nearly limitless. Costs are difficult to calculate. Defense is expensive. It often does not generate return on investment.

Now, most of us in this room today are what demographers are now calling digital immigrants, meaning that unlike my teenaged children, we were not born into the digital world that we now inhabit. Perhaps it is because cybersecurity economics is so foreign to us and is poorly understood at the consumer, national, and corporate levels.

For example, many consumers have a false sense of security due to their belief that most of the financial impact resulting from a loss of personal data will be fully covered by corporate entities, like the banks. In fact, much of these losses are transferred back to consumers in the form of higher interest rates and consumer fees. During the first panel, we talked about the prospect of a potential cyber hurricane, and the Federal Government does not seem to re-

alize that you are the de facto insurer of last resort. All of financial risk management is laid at the Federal Government steps right now because there is virtually no private cyber insurance market to help you.

Meanwhile, most of our corporate and Government structures are built on outdated models wherein the owners of the data do not understand themselves to be responsible for the defense of the data. The marketing department has data, the finance department has data, et cetera, et cetera, but they think the security of the data is the responsibility of the IT guys at the end of the hall. As a result, the financial risk management of cyber events across enterprise settings is not properly analyzed, not properly appreciated, and cyber defense is not adequately budgeted. The interaction of these factors may be at the root of the finding of the 2009 PricewaterhouseCoopers Global Information Security Study, which pointed out that, despite the increasing publicity about the dangers of cyber incursions, nearly half-–47 percent—of all enterprises are actually reducing or deferring budgets for information security initiatives. The ISA Social Contract, like the administration's Cyberspace Policy Review, argues that what will be required to address this issue is for the public sector to deploy market incentives to motivate private investment for the purposes of protecting the public interest.

Now, the good news, as we discussed during the first panel, is that the research shows that between 80 to 90 percent of cyber breaches could be prevented if we simply adopted the standards, practices, and technologies that we already have. The problem is we are not doing it.

The Government is charged with the responsibility to provide for the common defense, but in the cyber world, Government cannot do this alone. They will require the private sector cooperation and investment. While some of that investment will come from corporations serving their own private security needs, the extent of investment required to serve the broader public needs due to some of the unique aspects of cyber economics I just described will not be done.

In our written testimony, we provide a fairly comprehensive proposal how we can create a modern, sustainable, effective system of cybersecurity. However, to do this, we digital immigrants, including Members of Congress, may have to learn some new rules and some new language to manage this new world. We believe we can do it together.

Thank you, sir.

[The prepared statement of Mr. Clinton appears as a submission for the record.]

Chairman CARDIN. That gives us another reason for immigration reform.

Dr. Wortzel.

STATEMENT OF LARRY M. WORTZEL, PH.D., VICE CHAIRMAN, U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, WASHINGTON, DC

Mr. WORTZEL. Chairman Cardin, Ranking Member Kyl, thanks for giving me the opportunity to testify today.

Our Nation's critical infrastructure, economy, defense information, and citizens are threatened by hackers, terrorists, and hostile foreign intelligence services. Preventing computer network penetration and pursuing those who attack us while preserving privacy is a challenge. But I have to say our intelligence and law enforcement agencies have been recently successful in preventing terrorist attacks and detecting espionage because of the Foreign Intelligence Surveillance Act and the PATRIOT Act. I think with good legislation, vigorous oversight by Congress, and attention from the White House, our intelligence and law enforcement authorities can accomplish much in protecting America's computer networks.

In my remarks, I will make reference to the report Senator Kyl mentioned by the U.S.-China Economic and Security Review Commission on China's capability to conduct cyber warfare and penetrate and exploit computer networks. The report's findings are relevant to securing critical infrastructure and preventing cyber attacks. And the lessons learned by preventing intrusions from China apply to all other forms of intrusions.

In addition to discussing the Commission's findings about cybersecurity, I am going to provide my personal views, informed by my experience as an Army intelligence officer and my own research on the subject at The Heritage Foundation.

I think we can do better in some areas. I do not believe that the Computer Fraud and Abuse Act, even as amended by the PATRIOT Act, is sufficient to address some critical issues. One of these is the right of private response by individuals or corporations that may choose to retaliate against cyber intruders.

As our Commission's report documents, there have been significant penetrations of critical infrastructure, defense contractors, and Government cyber networks, including those of the Department of Defense and Congress. The Commission recommended that Congress respond by evaluating the effectiveness and the resources available for law enforcement and the intelligence community. Among the most important objectives should be developing reliable attribution techniques to determine the origin of computer intrusions. The Commission also recommended that Congress urge the Obama administration to develop measures to deter malicious Chinese cyber activity.

In a recent editorial, I pointed out that Government and private industry are still in a reactive posture to cyber intrusions and cyber espionage. And as yet, there is no fully coordinated Government and industry response. I think President Obama made a good start with the 60-day cyber review, but there still is no permanent cybersecurity coordinator at the White House, as recommended in its own review. Efforts to coordinate standards and policies across Government and in the private sector appear stalled without senior leadership in the National Security Council.

That said, I think President Obama was wise to incorporate the Homeland Security Council staff into the National Security Council. I think the National Security Act of 1947 is a fine model for the executive branch to address these things. I think with proper staffing in the White House, attention from the National Security Adviser, and the leadership in NSC meetings of the cabinet Secretary of the lead Department in the Executive branch, a unified,

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00033 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

well-led effort can bring together the agencies of the Government and coordinate cybersecurity with allies and private industry. Also, creating the U.S. Cyber Command is an outstanding initiative within the Department of Defense.

Now, there is still debate about what agency should lead cyber efforts and set standards. I think the Department of Homeland Security can help coordinate these with state and local governments as well as private industry.

I believe the lead agency for the government response however, should be the National Security Agency. NSA has a strong institutional culture of adherence to the Foreign Intelligence Surveillance Act. Its personnel are trained to protect the privacy and rights of American persons. No agency has the decades of experience the National Security Agency has in conducting operations in the electronic and cyber realms; its personnel are skilled and superbly trained; it has broad international contacts with allies and friendly governments; and it has wide contacts in the private sector. Also, it has got a cadre of highly skilled linguists who are able to work in the languages associated with foreign intrusions.

In closing, I think the Government should be able to set standards for private industry associated with the National Industrial Security Program. And with respect to our critical infrastructure, I think it would behoove us to insist on certain standards, particularly on things like utilities.

Thank you, gentlemen.

[The prepared statement of Mr. Wortzel appears as a submission for the record.]

Chairman CARDIN. Thank you for your testimonies. We will start with Senator Kyl.

Senator KYL. Thank you. Why don't I just take a couple of minutes here, because our first vote has started, and I want to apologize to all three of you. I found all of your testimony very important and useful, and it may be that we will want to follow up with some questions, if that is all right with you, because in about 10 minutes we will have to go to the vote.

I am still fixated a little bit on this question of who should lead the effort, and let me start, because you raised the question right at the end, Mr. Wortzel. You indicated you thought NSA would be the best to lead the overall effort, and if you could just give me about one more minute on that.

And then, Mr. Clinton, given that the interface with a lot of business is through the Department of Homeland Security, as you mentioned, how would that fit into an NSA with an overall lead?

And maybe, Mr. Nojeim, are there any concerns that you have with that kind of a structure, especially since another alternative would be military? But it seems to me that the Defense Department has its own kind of separate thing to do, but correct me if I am wrong.

Dr. Wortzel.

Mr. WORTZEL. Senator, I think you are absolutely right. With respect to the National Security Council, I tend to ask a couple of questions with to assess what the NSC might be doing.

First of all, there is no permanent senior director for cyber maters on the NSC. It looks like the acting senior director is pretty

well qualified for what he is doing. He comes out of the Department of Justice. But the White House needs to finalize this selection.

Now, the question looking at the NSC structure and effectiveness ought to focus on what happens if a deputies Committee meeting is held to make the highest-level recommendations to the President on cyber issues. What executive and department cabinet agency's deputy chairs it? I do not have the answer to that.

And I think the second question we should be asking is: Right now what is the highest level of executive out of the executive branch that has attended or chaired an NSC meeting on cyber issues? I am not even certain it is getting the right attention.

Now, I think no agency has better expertise maybe in the world than the National Security Agency broadly on electronic operations and operations in the electromagnetic spectrum. But at the NSC, the cabinet deputy chasing meetings should probably be the Deputy Attorney General. This puts the proper focus on privacy issues. I do not know if that is happening.

My own experience was as a very junior person with the senior interagency groups in the Reagan NSC. When we worked on counterintelligence matters, the Attorney General led it. When we worked on intelligence matters at the time, it was the CIA Director.

So I do not know what is happening on the NSC now. I do not see anything publicized about the processes. But those are the questions that have to be asked of the executive branch. I just do not think it is getting the right attention.

Mr. CLINTON. Senator, let me first start by commenting that I spend a lot of time suggesting that Members of Congress should not be telling the private sector how it should organize itself, so I am reluctant to tell the Federal Government how it should be organizing itself.

I think that the overall question, I would agree with Mr. Wortzel, about the need for attention is very important, and we think that the overall approach that the President articulated in May is correct in that the new cyber coordinator is supposed to have a dual-hatted responsibility both to the National Security Council and to the National Economic Council.

We think that this notion that cybersecurity is both a national security and a national economic security issue is critical. And so I would worry about turning over to NSA the leadership of this because I do not think that they take that sort of perspective. They have a very legitimate perspective, but I do not think it is that perspective.

I would also point out, as we indicated, we quote I think three different sources in our written testimony, and then NSA actually said in the previous panel that the vast majority of this stuff we already know how to do. He was saying 80 percent. Our research indicates up to 90 percent. So we do not need necessarily people to come up with in the main new programs and new—we know how to do a lot of this. We are just not doing it. Virtually everybody agrees on that.

Now, the other 10 to 20 percent of the problem, that is, like, really hard stuff, you know, and we definitely need a lot of work with

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00035 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

the NSA on that. The supply chain issues are enormous. There is a lot of work that needs to be done over there.

But in terms of creating the overall system, which is what we need, we need, as digital immigrants, as I say, we guys of our age quartile need to rethink how we are doing this. We cannot do this through cold war-era structures. And that is what we have now. We have the Department of Commerce, we have the Department of Justice. We are in these old structures. This does not make sense in the Internet age. We need to rethink this, and we need to rethink the approach.

So in the short term, I am happy with NSA doing a great deal of work on that other 10 percent. I would be reluctant to see them from their perspective take the leadership on the overall effort. My sense is that that should be run in a dual-hatted capacity out of the White House with a lot of work from DHS as well as, frankly, the Department of Commerce.

Chairman CARDIN. Thank you.

Mr. NOJEIM. May I add to those comments? Senator Kyl, I do not think NSA wants that role. The head of the NSA already said that it does not want to be in charge of cybersecurity. NSA might have particular expertise in finding attacks and identifying attacks. It can share that expertise with other agencies, civilian agencies, such as DHS. DHS has a lot of history in this area. It is not all good history. But it has got some new leadership, and I think you can have a lot of confidence in Phil Reitinger and his team. They seem to be tackling issues that had been left open for a while.

And I should add—I would be remiss if I did not—that NSA has certain baggage that it would bring to a leading role in the effort to secure civilian systems that other agencies do not have, including the warrantless wiretapping program.

Thank you.

Chairman CARDIN. Senator Whitehouse.

Senator WHITEHOUSE. Thank you. Given the status of the vote, I would probably make this a question for the record so that I do not keep us late. But I would like you, Mr. Nojeim, to get back to me on the boundary that you suggest between the provider-driven security measures in the private sector versus the Government-run national security protection measures. In light of what I would consider to be three—well, let us not call them "facts"—observations.

One, if, in fact, NSA has technical capabilities beyond those of the providers, why should you be relying on the providers in areas where NSA actually has greater capability?

Why should it be satisfactory to have NSA only brought in by the providers on an invite-in basis in circumstances in which the providers might not even know that a particularly sophisticated attack is underway through their systems, but NSA might?

And, finally, how can the relationship between the providers and NSA be anything but ongoing and routine when cyber attack is constant and unremitting? It is not like, OK, we are having some cyber attacks today and we will call in NSA, but today is a good day, we are not having cyber attacks today, so we do not need them.

We are under a constant, massive, unremitting barrage of cyber attack, and I do not see how you get out of ongoing and routine in that context.

Mr. NOJEIM. I will be happy to respond for the——

Senator WHITEHOUSE. I do not think we have time because of the vote.

Chairman CARDIN. If you could do it for the record, I think we would appreciate that. Unfortunately, there are a series of votes on the floor of the Senate; otherwise, we would try to keep the hearing moving forward. I think the point that Senator Whitehouse has raised, though, is of interest to all of us, so we would appreciate not just you, Mr. Nojeim, but if all of you would respond, we would appreciate it.

[The information referred to appears as a submission for the record.]

Chairman CARDIN. Mr. Clinton, I think your point about the economic issues is a very important point. I am curious as to how we can try to adjust that in the private sector and would welcome, I guess, more thoughts as to how we can adjust that. And, Dr. Wortzel, I think your comments about how we try to coordinate this is vitally important to our country.

We will keep the record open for additional questions by members of the Committee, and we thank all three of you for your testimony. It is a continuing effort, so we will look forward to your continued involvement as we try to get this right for our Nation.

With that, the Subcommittee will stand adjourned.

[Whereupon, at 11:45 a.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record.]

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00037 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

QUESTIONS AND ANSWERS

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 1, 2010

The Honorable Patrick Leahy
Chairman
Committee on Judiciary
United States Senate
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find responses to questions for the record stemming from the appearance of James Baker, Associate Deputy Attorney General, before the Committee on November 17, 2009, at a hearing entitled "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace."

We apologize for our delay in responding to your letter and hope that this information is helpful to the Committee. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosures

cc: The Honorable Jeff Session
Ranking Minority Member

Responses of the Department of Justice to Questions for the Record Arising from the November 17, 2009 Hearing Before the Senate Committee on the Judiciary Regarding Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace

Question from Senator Whitehouse

1. *Mindful of legitimate limitations on what the Executive Branch can and should disclose about sensitive cyber security initiatives, what sort of outreach, if any, [has DOJ] made to civil society groups on privacy and other civil liberties concerns? If you haven't made any such efforts yet, do you plan to? If not, why not?*

Response:

Because the private sector outreach aspects of the cyber security initiative are being developed and implemented by the Department of Homeland Security, the Justice Department has relied primarily on DHS to reach out to privacy and civil liberties groups to discuss the issue.

In addition, the Department of Justice (DOJ) has been actively involved in the Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC), led by the White House's National Security Staff (NSS). As part of our participation in that group, our Chief Privacy and Civil Liberties Officer attends a sub-IPC on Privacy and Civil Liberties issues. That sub-IPC is coordinating the Executive Branch's approach to these issues and its strategy for outreach from the U.S. government to private entities. The sub-IPC has solicited views from civil society groups on civil liberties and privacy issues related to implementation of certain cyber security initiatives. The Department will continue to participate in the sub-IPC to address such issues.

Questions from Senator Feingold

1. *Please answer the following questions to clarify the conclusions drawn by those opinions:*

    a. *Does the use of log-on banners or other computer-user agreements on executive branch computers completely eliminate employees' legitimate expectation of privacy in all of their Internet communications on those computers?*

b. If log-on banners or other computer-user agreements are used, do executive branch employees have any legitimate expectation of privacy when they access their personal (non-"dot gov"), password-protected email accounts on executive branch computers?

c. If log-on banners or other computer-user agreements are used, do executive branch employees have any legitimate expectation of privacy in any web browsing, Facebook messages, blog posts, Twitter posts or other forms of Internet communications that occur on executive branch computers?

d. If log-on banners or other computer-user agreements are used, is there any information on executive branch computers that may not be lawfully searched without a warrant?

e. Please specify whether the answer to any of these questions depends on the purpose of the government's search.

Response to Question 1, all subparts:

The Office of Legal Counsel ("OLC") opinions about the EINSTEIN 2.0 program conclude that with the adoption, implementation, and enforcement of the model log-on banners or computer user agreements described in the January 9, 2009 OLC opinion (or their substantial equivalents), federal employees do not have a reasonable expectation of privacy in their use of the government-owned information systems that are the subject of those banners or agreements with respect to the lawful purpose of protecting federal networks against intrusion and exploitation. *See* Memorandum Opinion for Counsel to the President, from Steven G. Bradbury, Principal Deputy Assistant Attorney General, Office of Legal Counsel, *Re: Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch* at 6-12 (Jan. 9, 2009) ("*January 9, 2009 Opinion*"); Memorandum Opinion for an Associate Deputy Attorney General, from David J. Barron, Acting Assistant Attorney General, Office of Legal Counsel. *Legality of Instrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch* at 2-3 (Aug. 14, 2009) ("*August 14, 2009 Opinion*"), both available at http://www.justice.gov/olc/allopinions.htm. That conclusion applies to such employees' web browsing activities and the content of any communications they send using government information systems, whether through a government email account or a personal, web-based, password-protected account such as Gmail, Hotmail, or Facebook accessed using the federal systems. *See January 9, 2009 Opinion* at 6-13; *see August 14, 2009 Opinion* at 3. The opinions further conclude that even if the employees' expectations of privacy were not entirely eliminated by the use of log-on banners or computer user agreements, the operation of the EINSTEIN 2.0 program nonetheless satisfy the reasonableness requirement of the Fourth Amendment. *See January 9, 2009 Opinion* at 16-21; *August 14, 2009 Opinion* at 4-5. *Cf. City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) (concluding that even if a municipal employee had an expectation of privacy in text messages sent to or from a

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00040 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.003

government pager, the review by the government employer of the employee's text messages did not violate the Fourth Amendment's reasonableness requirement, because the search was justified by a legitimate, work-related purpose and was reasonable in scope).

The EINSTEIN 2.0 program only scans the federal systems internet traffic of agencies that have deployed the program, and therefore, the OLC EINSTEIN 2.0 opinions did not need to address whether the government may lawfully obtain without a warrant information on executive branch computers that does not transit the federal systems network. Moreover, the purpose of the EINSTEIN 2.0 program is to protect the security of unclassified executive branch information systems from intrusion or exploitation, and for that reason, the OLC EINSTEIN 2.0 opinions similarly did not need to reach whether federal employees would have a reasonable expectation of privacy with respect to searches conducted for purposes other than cybersecurity.

2. ***In the course of its legal analysis, has the Department asked about the extent to which EINSTEIN 2.0 or other cybersecurity programs might be technologically engineered to impose a less onerous burden on the legitimate privacy interests of executive branch employees and third parties communicating with those executive branch employees?***

Response:

The design of the EINSTEIN 2.0 program as it relates to privacy interests is described in the Department of Homeland Security's *Privacy Impact Assessment for EINSTEIN 2.0* (May 19, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf. The legal analysis contained in the OLC EINSTEIN 2.0 opinions took into consideration the privacy-related design features that are described in that Privacy Impact Assessment, *see, e.g., January 9, 2009 Opinion* at 4 (noting that only data packets associated with malicious activity will be acquired and stored and that other packets will be deleted promptly, citing the DHS Privacy Impact Assessment for EINSTEIN 2.0), and concluded that the operation of the EINSTEIN 2.0 program struck a reasonable balance between any possible intrusion on the privacy interests of United States persons in the content of their Internet communications and the important governmental interest in protecting federal information systems from intrusion or exploitation, *see id.* at 20-21; *August 14, 2009 Opinion* at 4-5. I note also that the Supreme Court in *City of Ontario v. Quon* recently rejected the argument that a "reasonable" search for purposes of the Fourth Amendment must be the "least intrusive search practicable." 130 S. Ct. at 2632.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00041 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.004

3. ***In your testimony before the Committee, you stated that there are minimization procedures in place to ensure that "personally identifiable information or other information generated from [the EINSTEIN 2.0] program are handled appropriately." Please describe these minimization procedures in more detail.***

Response:

DHS created information-handling procedures that are currently being used in the operation and implementation of Einstein 2.0. However, DOJ did not have a role in developing or reviewing those procedures. Accordingly, specific questions regarding the application of Einstein 2.0's procedures are best directed to DHS.

4. ***In your testimony before the Committee, you stated that "not all the privacy issues with respect to EINSTEIN 2.0 have been resolved." Which privacy issues are yet to be resolved, and how does the Department of Justice intend to resolve those issues?***

Response:

The procedures that DHS created for the implementation of Einstein 2.0 contemplate that each agency will review its policies and practices, as well as the law, to determine whether it needs to direct DHS to adopt any special procedures for managing the agency's data. We understand this agency-by-agency review will be an ongoing process during the implementation of Einstein 2.0 and is still underway at agencies that are enrolling in the Einstein 2.0 program, including the Department of Justice.

5. ***In May, Lt. General Keith Alexander testified as follows to the House Armed Services Committee: "Traditionally, military action is an option of last resort that should complement deterrence strategies. Within the DoD, deterrence can be partially achieved through the creation and maintenance of a cyber force capable of freely operating within cyberspace." Please describe any Department of Justice legal analyses related to the Department of Defense's cyber capabilities.***

Response:

The Department of Justice works regularly with the Department of Defense on a wide variety of legal and policy issues, including cybersecurity-related matters. Unfortunately, I am not able to elaborate more fully in response to your question in an unclassified setting.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00042 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.005

Questions from Senator Hatch

1. ***The PRO-IP Act specifically provides that all CHIP units are to be assigned at least two AUSAs responsible for investigating and prosecuting computer hacking or intellectual property crimes. Considering the seriousness of these crimes, I would have preferred dedicating a specific number of AUSAs to prosecuting criminal intellectual property crimes and having others focused on prosecuting and investigating computer hacking crimes. Do you agree with this idea?***

Response:

Maintaining CHIP AUSAs' dual responsibilities over prosecuting both computer crime and IP offenses is an important and effective way to maximize their knowledge and expertise to the benefit of each of those areas. Since 1995, the CHIP Network has evolved into an effective group of prosecutors who specialize not only in prosecuting computer crime and IP offenses but who also have developed a unique expertise in the types of investigative tools and techniques necessary to prosecute these crimes. The tools used in obtaining electronic evidence, reviewing forensic analysis, and pursuing online investigations overlap for both the computer crime and IP areas. In addition, there are certain IP and computer crime offenses which occur during the same criminal act. For example, a criminal who misappropriates a trade secret often does so in violation of computer intrusion laws. In this regard, a prosecutor who pursues IP crimes will necessarily be more effective in prosecuting computer crimes. In addition to working on their own cases, the CHIP prosecutors are able to contribute their expertise in these areas as legal advisors to other prosecutors in the office confronting similar issues.

2. ***Can you give me an estimate of how much time CHIP prosecutors devote to cyber security related crimes compared to IP-related crimes?***

Response:

The Department does not maintain data that describes the allocation of time each CHIP prosecutor spends on cybersecurity as compared to IP crimes. Nor can a general comparison be made, as the focus of a particular CHIP Unit will depend on the types of crimes that are more prevalent in that District. That said, DOJ recognizes the importance of vigorous enforcement of cybercrime laws and devotes substantial resources to ensuring adequate support for the investigation and prosecution of such offenses.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00043 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.006

Questions from Senator Kyl

1. ***While there are many aspects of cyber security, please describe the major focus of your department's involvement in the cyber security field.***

Response:

As described more fully in my testimony, the Department's involvement in the cybersecurity field primarily includes the following: (1) enforcing criminal laws that help secure our data and computers; (2) facilitating the domestic collection of foreign intelligence information, including intelligence that supports cybersecurity efforts; (3) providing legal guidance within the Executive Branch related to the unique challenges posed by threats in cyberspace, on topics ranging from the use of existing legal tools and authorities, the legality of cybersecurity programs like the EINSTEIN program, and the ways in which we can most vigorously protect privacy and civil liberties while still achieving our goal of securing the Nation's information infrastructure; (4) working closely with our partners throughout the government to inform cybersecurity-related policy discussions; and (5) securing our own agency's networks.

2. ***What future roles is your department best suited to focus on in the cyber security field?***

Response:

We anticipate that we will continue to devote significant effort and resources to the areas listed above to expand our growing expertise in all of these areas. We have had successes on all of these fronts and are constantly looking for opportunities to build upon those successes.

3. ***Please share any concerns you have about the security of government or private computer systems that are currently not part of your department's mission or authority.***

Response:

As you are aware, the threats we face are varied and evolving. For a variety of reasons, data breaches and other types of cyber threats are significantly underreported, and as a result, law enforcement efforts to investigate intrusions and bring criminals to justice can be significantly hampered. Securing the data on private sector networks is not itself part of the Department's authority, but we will continue to work with and support other government agencies on that important issue. Immediate reporting of incidents to law enforcement, however, is vital to law enforcement's ability to investigate large-scale data breaches and other dangerous intrusions. There is currently no federal requirement that companies report breaches

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00044 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.007

to federal law enforcement. As a result, we urge Congress to consider requiring security breach reports to federal law enforcement using a mechanism that ensures that the United States Secret Service and the FBI have access to the reports.

4. ***Please describe the cyber-security measures your department is considering that are currently affected by legal restrictions.***

Response:

Virtually all cybersecurity measures that the government considers taking are impacted in some way by the existing federal legal framework. In particular, the Department has looked at issues regarding the authorities of various federal agencies to undertake particular cybersecurity activities, such as the EINSTEIN program, as well as legal restrictions on such activities, such as the Electronic Communications Privacy Act of 1986, as amended (ECPA). The Department has also evaluated laws such as ECPA that limit the sharing of cybersecurity information.

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is the primary statute that the Department uses to prosecute and deter computer intrusions. While it is generally effective, a number of targeted amendments could enhance its efficacy by enhancing its penalty provisions and closing loopholes. In addition, Congress could correct several shortcomings that were introduced last year when section 1030 was amended by the Identity Theft Enforcement and Restitution Act of 2008 (ITERA). We would be happy to discuss these potential amendments with you.

5. ***Cyber threats to government and private systems are rapidly evolving. Are there specific concerns you have about your department's ability to perform its mission effectively in the future?***

Response:

The Department is taking steps to ensure that we can continue keeping pace with rapidly evolving cyber threats to government and private systems. Again, ensuring that we have the resources and investigative tools in place to keep pace with emerging technologies and developments in the threat environment is critical to our ability to continue to perform our mission effectively in the future.

6. ***Are there areas where Congressional action may soon be necessary to prevent dangerous vulnerabilities? If yes, please describe.***

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00045 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.008

Response:

We look forward to continuing to work with Congress to determine whether action may be needed. We cannot describe particular vulnerabilities in this setting.

7. ***Is your department taking any steps specifically to address international cyber threats to government and private systems?***

Response:

Yes. As discussed more fully in my testimony, the Department is working closely with our international partners through our work on and support of the Convention on Cybercrime, our status as the United States' Point of Contact in the G8 High-Tech Crime's 24/7 network, and our efforts to train hundreds of domestic and foreign law enforcement agents on the legal tools we use in our enforcement efforts. In addition, we have provided significant support – through legal guidance – to those responsible for the U.S. Government's development of the EINSTEIN program, and we work closely with our international law enforcement partners on individual cyber cases. These partnerships have resulted in successful prosecutions both here and abroad that have made our country safer from international cyber threats.

8. ***How many cyber cases in 2008 concerned attacks from China?***

Response:

As the Committee is aware, attack attribution is one of the most vexing problems in conducting cyber investigations. As a result, it is difficult to answer this question with precision. Further, this question is more appropriately directed at the FBI or other federal agencies with responsibilities in this area. That said, in his Annual Threat Assessment issued earlier this year, the Director of National Intelligence (DNI) described China's cyber activities as "aggressive." Based upon information available to us, we would concur in the DNI's assessment. *See Annual Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence*, February 3, 2010, *available at* http://www.odni.gov/testimonies/20100203_testimony.pdf

9. ***What is the nature of DOJ's interaction, if any, with Chinese authorities regarding cyber cases?***

Response:

The Department has, in recent years, greatly developed its relationship with Chinese authorities regarding some crimes that have a cyber aspect. The Department, through its Criminal Division, co-chairs the Intellectual Property Criminal Enforcement

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00046 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.009

Working Group (IPCEWG) and the Cybercrime Working Group of the U.S.-China Joint Liaison Group for Law Enforcement Cooperation (JLG). The IPCEWG has fostered an open dialogue on criminal intellectual property enforcement, increased information and evidence sharing, and resulted in a number of successful joint intellectual property operations, including Operation Summer Solstice, which targeted a criminal organization believed to be responsible for the distribution of over $2 billion worth of pirated and counterfeit software and was the largest-ever joint criminal enforcement operation between the FBI and the Chinese Ministry of Public Security. Similarly, the Cybercrime Working Group has established a dialogue on Chinese and U.S. substantive and procedural law related to cybercrime investigations, including evidence sharing practices and investigative capabilities. To date, there have not been any joint enforcement actions in cybercrime investigations. However, case investigative referrals and informal requests for assistance have been exchanged through the JLG and police-to-police channels.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00047 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.010

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 13, 2010

The Honorable Patrick Leahy
Chairman
Committee on Judiciary
United States Senate
Washington, D.C. 20515

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of FBI Cyber Division Deputy Director Steven Chabinsky, before the Committee on November 17, 2009, at a hearing entitled "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace."

We apologize for our delay in responding to your letter and hope that this information is helpful to the Committee. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosures

cc: The Honorable Jeff Session
Ranking Minority Member

Responses of the Federal Bureau of Investigation to Questions for the Record Arising from the November 17, 2009, Hearing Before the Senate Committee on the Judiciary Regarding Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace

Questions Posed by Senator Whitehouse

1. Mindful of legitimate limitations on what the Executive Branch can and should disclose about sensitive cyber security initiatives, what sort of outreach, if any, have your respective agencies made to civil society groups on privacy and other civil liberties concerns? If you haven't made any such efforts yet, do you plan to? If not, why not?

Response:

As a matter of practice, the FBI routinely engages with outside entities that may have significant interests in the development of FBI policy. For example, the FBI reached out to privacy and civil liberties groups during the development of the N-DEx program and to Muslim organizations, among others, during the development of our internal policy guidance on the implementation of the Attorney General Guidelines for the conduct of investigations. The FBI also has its own Privacy and Civil Liberties Officer who consults on all key initiatives that may have an impact on privacy and civil liberties and helps to ensure that the views of outside advocates are analyzed as part of any project development. Privacy interests are also protected by the FBI's compliance with the Fair Information Practices embodied in the Privacy Act, which govern the collection, use, maintenance, and dissemination of personally identifiable information and apply to all Federal agencies. Finally, the FBI also keeps current on international privacy norms, including the Madrid Privacy Declaration, which was recently agreed to by over 100 civil society organizations. The majority of the policies expressed therein are already followed by the Department of Justice (DOJ), including the FBI.

Questions Posed by Senator Hatch

Cyber Terrorist Attacks

2. Deputy Assistant Director Chabinsky, as you are aware terrorist groups today frequently use the Internet to communicate, raise funds, and gather intelligence on future targets. Although there is no published evidence that computers and the Internet have been used directly, or targeted in a terrorist attack, malicious attack programs currently available through the Internet can allow anyone to locate and attack networked computers that have

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00049 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.012

security vulnerabilities, and possibly disrupt other computers without the same vulnerabilities.

Terrorists could also use these same malicious programs, together with techniques used by computer hackers to possibly launch a widespread cyber attack against computers and information systems that support the U.S. critical infrastructure.

In a press interview last April, Secretary of Defense Robert Gates said that the U.S. is "under cyber attack all the time, every day." Can you roughly estimate how many cyber terrorist attacks does the FBI investigate on an annual basis?

Response:

The response to this inquiry is classified and is, therefore, provided separately.

Terror Fighting Tools in Investigating Cyber Communications

3. Deputy Assistant Director Chabinsky, setting aside the widespread cyber attack for a moment, I am also concerned about how technology is making it easier for terrorists to communicate. Smart phones have become hand held computers that make phone calls and transmit email. Laptops with wireless internet can operate in city parks, fast food restaurants and coffee shops. Some in Congress want to raise the requirements and increase burdens of proof for the FBI before they can gather information on suspected terrorists. I am not one of those people especially when I have seen the numbers on how often they have been used and how successful they have been.

a. Would the FBI use 215 business records searches to gain information on a particular ISP or if a Wi-Fi hot spot that had been repeatedly used? I ask this because the Senate will be debating the reauthorization of the PATRIOT Act. These are critical tools that Director Mueller has publicly endorsed as essential in detecting terrorist plots.

b. If possible, can you elaborate on how the Cyber Division uses terror fighting tools when terrorists retreat to cyber communication?

Response to subparts a and b:

Consistent with the Attorney General's Guidelines for Domestic FBI Operations and the FBI's associated Domestic Investigations and Operations Guide, in deciding what investigative techniques to use in a given case, the FBI considers which techniques will afford an effective and efficient means of accomplishing the investigative objectives in the least intrusive manner based on all of the circumstances involved. The FBI would apply for an order under the Foreign Intelligence Surveillance Act (FISA) Business Records provision in the referenced circumstances if that would be the most timely, most effective, and least intrusive means of investigating a suspected terrorist.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00050 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.013

Questions Posed by Senator Kyl

Please respond to the following questions. If any of the questions below require classified answers, please provide them in classified form.

4. While there are many aspects of cyber security, please describe the major focus of the FBI's involvement in the cyber security field.

Response:

Pursuant to the roles and responsibilities articulated in the National Strategy to Secure Cyberspace and the Comprehensive National Cybersecurity Initiative (CNCI), the FBI leads the National Cyber Investigative Joint Task Force, a presidentially mandated focal point through which government agencies coordinate, integrate, and share information related to domestic cyber threats. The FBI's Cyber Division manages investigations into computer intrusions targeting the national information infrastructure and into other significant Internet-facilitated criminal activities, many of which have international facets and broad economic implications.

While protecting the freedom, privacy, and civil liberties of Americans, the FBI's strategy focuses on identifying and disrupting:

- The most significant individuals, groups, and foreign powers conducting computer intrusions, disseminating malicious code, or performing other criminal computer-supported operations. This includes the FBI's focus on cyber-based terrorism and hostile foreign intelligence operations conducted over the Internet against domestic targets .
- Online predators or groups that sexually exploit and endanger children for personal or financial gain.
- Operations targeting U.S. intellectual property.
- The most significant perpetrators of Internet fraud affecting domestic interests.

While the FBI's primary focus is on reducing the cyber *threat* level (that is, neutralizing the actors, themselves), the FBI's threat-based investigations also provide a wealth of information that is used by the *vulnerability mitigation* community and the *consequence management* community. The FBI exchanges cyber threat and crime information with a number of national cyber centers, including the Department of Homeland Security's United States Computer Emergency Readiness Team, which mitigates threats against Federal and private sector networks. The FBI has developed a robust cyber intelligence analysis

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00051 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.014

capability which, combined with mature dissemination processes, provides a full-spectrum approach to cyber risk management and shared situational awareness. Through these different programs, the FBI endeavors to ensure that the information it collects is used for all relevant cyber security purposes, and not just to further FBI investigations.

5. What future roles is the FBI best suited to focus on in the cyber security field?

Response:

In addition to enhancing its current ability to keep pace with evolving technologies, the FBI is well suited to continuing its efforts, in coordination with other Federal agencies, to ensure that: 1) industry requirements for understanding the current threat level are fully addressed; 2) predictive warnings are provided in as timely a manner as possible to the greatest possible number of stakeholders; and 3) the private sector's response to major incidents involving data breaches and intrusions into process control systems includes timely referral to the FBI. The FBI is also well suited to delivering its specialized cyber training capabilities and curriculum to our domestic and international law enforcement partners.

6. Please share any concerns you have about the security of government or private computer systems that are currently not part of your department's mission or authority.

Response:

The defensive "information security" aspects of cyber security require sustained investment in technology, systems testing and log auditing, and user education and compliance. Current network configurations are always vulnerable to the "weakest link," and a single corrupted computer or human error can impact the security posture of an entire network.

7. Please describe the cyber-security measures your department is considering that are currently affected by legal restrictions.

Response:

All FBI investigations are conducted pursuant to Constitutional, statutory, and policy restrictions, many of which are designed to protect civil liberties and privacy. These include the Fourth Amendment, the Privacy Act, the Electronic Communications and Privacy Act, and FISA. For example, as described in the DOJ manual entitled, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," the law governing electronic evidence in criminal investigations has two primary sources: the Fourth Amendment to the U.S. Constitution and the privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00052 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.015

8. Cyber threats to government and private systems are rapidly evolving. Are there specific concerns you have about your department's ability to perform its mission effectively in the future?

Response:

The FBI continues to pursue the strategy articulated in the CNCI in order to address the rise in terrorist, nation-state, and criminal network attacks and compromises. While the FBI seeks to improve its ability to address the evolving and increasing cyber threat through the strategic deployment of its cadre of skilled and trained cyber agents, analysts, and forensic examiners, we are concerned that changes in technology may limit our future inability to capture the communications and cyber attack-related activities of our adversaries.

9. Are there areas where Congressional action may soon be necessary to prevent dangerous vulnerabilities? If yes, please describe.

Response:

Dangerous vulnerabilities exist throughout the government and the private sector and the FBI anticipates that systems containing these vulnerabilities will persist within our critical infrastructure for the foreseeable future. Both government and private sector systems continue to deploy new technologies without having in place adequate hardware or software assurance schemes or security processes that extend through the entire network life cycle.

10. Is your department taking any steps specifically to address international cyber threats to government and private systems?

Response:

DOJ is working closely with its international partners to address international cyber threats, including through its work on and support of the Convention on Cybercrime, its status as the United States' point of contact in the G8 high-tech crime's 24/7 network, and its efforts to train hundreds of domestic and foreign law enforcement agents on the legal tools used in enforcement efforts. DOJ provides international training and technical assistance with the use of foreign assistance (INCLE) funds provided by the State Department's Bureau for International Narcotics and Law Enforcement Affairs. In addition, DOJ has provided legal guidance to those responsible for the U.S. Government's development of the EINSTEIN program, and it works closely with international law enforcement partners on individual cyber cases. These partnerships have resulted in successful prosecutions both domestically and abroad that have made our country safer from international threats.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00053 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.016

The Strategic Alliance Cyber Crime Working Group (SACCWG) was formed to build on strong multilateral relationships between the United States, United Kingdom, Canada, Australia, and New Zealand. Recognizing that traditional methods of investigating cyber crime are becoming obsolete in the face of new technologies and the numerous obstacles to policing cyber crime, the SACCWG works to address international cyber threats through collaborative investigations and shared intelligence.

The success of the FBI's transnational partnerships is exemplified by last year's case involving Worldpay, the credit card processing division of the Royal Bank of Scotland. In this case, a transnational crime organization used sophisticated hacking techniques to withdraw, in less than 12 hours, over $9 million from 2,100 automated teller machines in 280 cities around the world including Hong Kong and cities in the United States, Russia, Ukraine, Estonia, Italy, Japan, and Canada. This investigation and its related work with international law enforcement authorities resulted in multiple arrests throughout the world.

The FBI's "Operation Phish Phry" is another recent example of the many successful relationships between the FBI and our Federal, state, local, international, and private sector partners. Phish Phry resulted from ongoing coordination efforts between the FBI and United States financial institutions. Through the course of this two-year investigation, Phish Phry uncovered thousands of victims and at least $1.5 million in theft, identifying a sophisticated international computer intrusion, identity theft, and money laundering scheme comprised of hundreds of identified subjects in the United States and Egypt. Phish Phry, which was the first joint cyber investigation by Egyptian law enforcement authorities and the FBI, led to a 51-count Federal indictment charging 53 U.S. citizens and to the identification by Egyptian law enforcement authorities of 47 Egyptian suspects.

These recent international successes have encouraged the FBI's Cyber Division to embed investigators in national police agencies in the Netherlands, Estonia, Ukraine, and Romania. The FBI anticipates that this coordination will further enable us to leverage partner resources and relationships to aid in the fight against international cybercrime.

11. In your testimony, you talked about the FBI's success in countering cybercrime, but only after noting that "our networked systems have a gaping and widening hole in the security posture of both our private sector and government systems."

a. Where is the FBI losing ground?

Response:

The cyber attack and espionage capabilities of our foreign adversaries is outpacing the FBI's ability to adequately predict their plots and prevent their success.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00054 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.017

b. What is the FBI doing to close the gap?

Response:

In the broadest sense, the FBI's ability to respond to these challenges depends on our efforts to: improve the recruitment, selection, and retention of cyber personnel, continuously develop the skills and abilities of the FBI workforce and the technology used, identify and develop leaders with cyber expertise, build and strengthen strategic partnerships with internal and external partners to improve response to cyber threats, and maximize the role of technology when it can enhance mission effectiveness.

More narrowly, the FBI works to close the gap by pursuing the strategy articulated in the CNCI. This includes:

- Identifying "requirements" (what we must know to safeguard the nation).
- Providing planning and direction (to include strategic management of the investigative process).
- Conducting lawful collection (through such activities such as interviews, technical and physical surveillance, human source operations, and property searches).
- Engaging in timely information processing and exploitation (to convert the vast amounts of digital information collected to a form usable by analysts).
- Promoting rigorous analysis and production (converting raw information into actionable intelligence that is integrated, evaluated for reliability and relevance, and analyzed in context, and offering conclusions regarding its implications).
- Providing wide dissemination to ensure the effective distribution of raw and finished intelligence to the consumers who need it.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00055 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.018

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY & TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

December 11, 2009

The Honorable Sheldon Whitehouse
United States Senate
502 Hart Senate Office Building
Washington, D.C. 20510

Re: Answers for the Record to Questions Posed at 11/17/09 Cybersecurity Hearing

Dear Senator Whitehouse:

We are very pleased to respond to the questions you posed for the record at the November 17, 2009 cybersecurity hearing before the Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security. You asked three questions about the role of the National Security Agency in securing private networks.

Background on NSA's Role in Cybersecurity

Before answering your specific questions, we wanted to provide further context for our views.

Over 85% of critical infrastructure information systems are owned and operated by the private sector. The private sector has tremendous incentives to protect its own systems and devotes consider effort to doing so. Consequently, private sector network operators have a wealth of information about vulnerabilities, exploits, patches and responses that might be useful to the government. However, private sector operators may hesitate to share this information with the government if, because of a lack of transparency, they do not know how it will be used and whether it will be shared with competitors who might exploit it.

The NSA is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the kind of information sharing necessary for the success of a cybersecurity program. If an intelligence agency such as the National Security Agency were to take a lead role in securing civilian systems, it almost certainly would mean less trust among parties – and trust is essential to success of the program. It can result in less corporate and public participation, increasing the likelihood of failure or ineffectiveness of the cybersecurity program.

Mistrust of the NSA in particular relates in part to its recent involvement in secret eavesdropping activities that failed to comply with statutory safeguards. In the

P +1-202-637-9800 F +1-202-637-0968 E info@cdt.org

Terrorist Surveillance Program, as you well know, the NSA eavesdropped on communications between people in the U.S. and people abroad without the court order that FISA required. The legal ambiguity around the TSP, and the NSA's apparent willingness to act in contravention of statutory standards, placed private sector companies asked to assist with the surveillance in an extremely difficult position; those that provided assistance were exposed to massive potential liability. Given NSA's very recent history of acting outside statutory limits, the private sector and the public at large may not willingly share or expose cybersecurity information to the NSA no matter what statutory safeguards seem to be established around it.

The better approach, to the extent that the NSA has special expertise in cybersecurity, is to develop the means for ensuring that such expertise is made available to private sector network operators, so that they can better protect their own systems.

Specific Questions

Responses to your specific questions about the NSA's role in securing private networks are set forth below.

1) To the extent that NSA has unique technical capabilities compared to private-sector providers, why not rely on NSA to furnish security in areas where those capabilities may provide superior protection against cyber threats?

As a general rule, private sector providers know their own systems best, and know best how to secure their own systems. Security is critical to the survival of their businesses. So far, we have seen no public evidence that NSA could do a better job than could the providers who work 24 hours/day to secure their networks. So the first step is to identify – publicly to the maximum extent possible – any areas in which the NSA in fact has unique expertise that it cannot share with the makers and operators of communications equipment and systems.

Our primary concern is that the furnishing of security by NSA would entail NSA monitoring private-to-private communications. When network providers monitor their own systems for security purposes, they often must access communications content to provide security. The Electronic Communications Privacy Act permits network operators to do this to protect their networks. If, instead, NSA were to provide these services, it would likely have to access communications content, to the detriment of consumer privacy, and in direct contravention of ECPA.

To the extent NSA has unique technical capabilities that private sector providers lack, it should share those capabilities with providers through U.S. CERT or other avenues to help providers secure their networks. For example, NSA has attack signatures that providers lack. We have been told that NSA often classifies these attack signatures and does not share them. Instead of having NSA monitor private-to-private communications as a result of this problem, Congress should consider ways to ensure that providers have personnel who are cleared to receive such information, protect it against disclosure, and use it effectively.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00057 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.020

2) How could a system whereby NSA employs these capabilities to defend private-sector providers solely by the invitation of those providers function effectively when the providers might not even know that a sophisticated attack is under way, whereas NSA might?

If NSA were monitoring the system of a private sector provider and discovered an attack that the private sector operator would not have otherwise discovered, the NSA would have to tell the provider the secret information that only NSA had, so the provider can stop the attack. Precious time could be lost while NSA explains to the private sector operator what NSA believes is an attack and the private sector operator explains its network to the NSA in order to confirm that an attack is indeed occurring. (Both the NSA in protecting government systems, and private sector operators in protecting their systems, experience many alarms that require further examination, after which they are often determined to be false alarms.) It would be preferable for NSA to arm the private sector operator in advance with the information and techniques that would allow the private sector operator to more quickly respond to sophisticated attacks.

We agree with you that it would not be effective to employ NSA's capabilities only at the invitation of providers, but we do not thereby conclude that NSA should ubiquitously become involved in securing private sector networks. Instead, there should be on-going coordination between the NSA and the private sector through U.S. CERT, the ISACs or other means. U.S. CERT has already become a trusted information clearinghouse for threat and vulnerability information and NSA should be one of the entities that feeds information into that clearinghouse on an ongoing basis.

Using a mechanism such as U.S. CERT to disseminate NSA information may have the further advantage of "anonymizing" NSA as the source of the information. Often, it would seem that the legitimate secrecy concern of NSA would not be the knowledge that a particular vulnerability is being exploited; rather, the secrecy interest is in protecting NSA as the source of that knowledge. Likewise, as mentioned above, while NSA should share attack signatures with private sector providers on a secured basis, further thought might be given to what is the best mechanism for protecting NSA as the source of the knowledge of those signatures. Surely, if an attack signature is "compromised," the adversary using that signature will know that it is no longer working, whether the NSA or a private sector entity is neutralizing the attack.

3) Indeed, how can the relationship between providers and NSA be anything but ongoing and routine when cyber attack is constant and unremitting?

What concerns us is not an on-going relationship, *per se*, between the providers and the NSA through U.S. CERT. Rather, what concerns us is the prospect of ongoing, routine disclosure of private-to-private communications for cybersecurity reasons to NSA or to another agency of the federal government. The question is not whether the NSA should provide ongoing assistance – the question is what should be the nature of that assistance. Where we draw the line is against inserting the NSA, or any other government entity, into the flow of traffic on a private sector network. Most providers effectively handle most attacks day in and day out, and do not need to make ongoing disclosure of

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00058 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.021

traffic to NSA or to another agency of the government in order to protect their networks against those attacks.

We deeply appreciate your thoughtful approach to this issue, and we hope this information is helpful to you. Please do not hesitate to contact me if you would like to discuss further these or other cybersecurity matters.

Sincerely,

Gregory T. Nojeim
Director, Project on Freedom, Security and Technology

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00059 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.022

Question#:	1
Topic:	outreach
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

Philip Reitinger, NPPD Undersecretary

Question: Mindful of legitimate limitations on what the Executive Branch can and should disclose about sensitive cyber security initiatives, what sort of outreach, if any, have your respective agencies made to civil society groups on privacy and other civil liberties concerns? If you haven't made any such efforts yet, do you plan to? If not, why not?

Response: The Department of Homeland Security (DHS) puts privacy and civil liberties considerations at the center of its cybersecurity efforts. This approach is consistent with statutory imperatives contained in the Homeland Security Act, and it conforms to the President's recent remarks regarding the contours of national efforts to improve cybersecurity while protecting the privacy of Americans. The DHS Privacy Office serves as the steward of the laws and policies that protect the collection, use, and disclosure of personal and Departmental information. The Department recognizes the increasing need to approach cybersecurity holistically and in ways that further coordinate with the privacy community.

In this capacity, the Chief Privacy Officer has organized multiple briefings for the privacy community regarding the development of DHS's cybersecurity effort. Moreover, DHS created the Data Privacy and Integrity Advisory Committee (DPIAC) which advises the Secretary of the Department of Homeland Security and the Department of Homeland Security Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within the Department that affect individual privacy, as well as data integrity and data interoperability and other privacy related issues. The DPIAC is comprised of members from the Privacy and Civil society groups.

Recognizing the need to encourage and continue a civil liberties and privacy dialogue surrounding cybersecurity activities, DHS's Office of Cybersecurity and Communications, its National Cyber Security Division, and the DHS Privacy Office hosted recognized members of the civil liberties and privacy community on three occasions over the past year.

DHS held a meeting on September 1, 2009, with representatives of privacy and civil liberties groups at a classified level to discuss, in depth, the concept of operations and architecture of an exercise tied to the EINSTEIN 3 program. The purpose of the exercise is to demonstrate an intrusion prevention system technology capable of detecting and blocking malicious activity on the network of a Federal Civilian Executive Branch Department or Agency. This exercise is integral to the program development and design

Question#:	1
Topic:	outreach
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Sheldon Whitehouse
Committee:	JUDICIARY (SENATE)

of the EINSTEIN 3 architecture, providing test results of privacy protection processes that will help the Department ensure adherence to all privacy and civil liberties mandates and guidelines. DHS provided the privacy and civil liberties groups with the status of exercise kick-off activities and highlighted significant civil liberties and privacy protection accomplishments. This was a follow-on engagement to a March 26, 2009, event where DHS met with some of the same civil liberties and privacy community members. At that meeting, DHS provided briefings and supported discussions, again at a classified level, to familiarize attendees with EINSTEIN technology and DHS cybersecurity programs. At that meeting, there was a special focus on civil liberties and privacy implications, plans and activities.

A third meeting with privacy community members was held on December 2, 2009 during which DHS and community members discussed the EINSTEIN 3 exercise in detail.

Question#:	2
Topic:	best practices
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

Question: Mr. Reitinger, computer virus incidents cost companies billions of dollars every year. While antivirus technologies for detection and containment are attempting to keep pace, the threat is constantly evolving. The attack vector is no longer simply an infected executable on a floppy disk. Email, websites, macro-enabled documents, instant messages, peer-to-peer networks, cell phones, and other interconnected systems are all potential entry points onto our networks for a wide range of malware.

To successfully defend these entry points, as well as recover in the event of a given contamination, needs improvement. As we have seen critical private sector and government networks are often inter-dependent on each other. When offending networks are identified, how does DHS know that best practices were used to isolate the carrier? Where can private entities go to receive guidance on best practices?

Response: The National Institute of Standards and Technology (NIST) provides a comprehensive list of best practices documented in their Special Publication Series for use by public and private sectors. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) has contributed to the development of some of these publications in addition to other NIST Programs such as the National Vulnerability Database (NVD).

In the event that US-CERT becomes aware of a possibly malicious internet protocol (IP) address, it does not and cannot isolate a carrier. Instead, it shares this information with its partners so that they may take the necessary protective steps to prevent or mitigate exploitation from that IP address. US-CERT shares best practices and relevant information in mitigating threats or vulnerabilities when it has that information.

Under the Federal Information Security Management Act of 2002 (FISMA) and its associated authorities, each Federal Civilian Executive Branch Department and Agency is required to inventory its major information systems, to identify and provide appropriate security protections, and to implement an agency-wide information security program.

With respect to non-Federal entities, US-CERT and its parent organization, the National Cyber Security Division (NCSD), are available to provide technical assistance upon request to State, local and private-sector partners. US-CERT also maintains a public-facing website and a secure portal which together serve as a clearinghouse for cybersecurity risk data and mitigation information. The public-facing US-CERT website (http://www.us-cert.gov/) offers security tips, tools, techniques, vulnerability information,

Question#:	2
Topic:	best practices
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Orrin G. Hatch
Committee:	JUDICIARY (SENATE)

and recommended practices to enhance cybersecurity. The secure portal provides a secure, web-based, collaborative environment that enables government and private-sector partners to share sensitive, cyber-related information and news among one another.

Question#:	3
Topic:	focus
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: While there are many aspects of cyber security, please describe the major focus of your department's involvement in the cyber security field.

Response: The Department of Homeland Security (DHS) has multiple responsibilities for U.S. cybersecurity that cut across a wide range of substantive areas. Broadly speaking, DHS focuses its cyber security efforts on ensuring that the information and communications infrastructures that support civil government and the critical infrastructure and key resource sectors are safe, secure, trustworthy, and resilient. It does so through the coordinated efforts of several departmental components.

First, the Office of Cybersecurity and Communications (CS&C) within the National Protection and Programs Directorate (NPPD), serves as the Department's primary focal point for the security of cyberspace. In collaboration with other Federal departments and agencies with cyber expertise, including, *e.g.*, the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, CS&C facilitates interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. CS&C's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems; to the extent permitted by law, the organization also supports the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace. In addition to CS&C, the National Cyber Security Center (NCSC) within NPPD—when it reaches full operational capability—will also help to secure U.S. Government networks and systems by coordinating and integrating information among the national cybersecurity centers to provide cross-domain situational awareness, and analyzing and reporting on the composite state of the U.S. Cyber Networks and Systems and fostering collaboration.

Several components outside of NPPD also contribute to DHS's cybersecurity mission responsibilities. For instance, the U.S. Secret Service and U.S. Immigration and Customs Enforcement (ICE) have law enforcement responsibilities related to aspects of cybercrime; the DHS Privacy Office assesses departmental cyber security efforts to minimize their potential privacy impact on individuals; the DHS Science and Technology Directorate has research and development responsibilities in the area of cybersecurity and critical infrastructure protection; and the DHS Chief Information Officer is the lead for ensuring DHS's networks and systems are secure. The DHS Office of Intelligence &

Question#:	3
Topic:	focus
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Analysis (I&A) is responsible for identifying and assessing cyber threats and providing timely, accurate, and actionable intelligence to Federal civilian departments and agencies; State, local, and tribal authorities; and to the owners and operators of the nation's Critical Infrastructure/Key Resources. To ensure a coordinated approach to cyber security across government, the Department works closely with the U.S. Chief Technology Officer, the U.S. Chief Information Officer and, soon, with the incoming White House Cybersecurity Coordinator.

Question#:	4
Topic:	roles
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: What future roles is your department best suited to focus on in the cyber security field?

Response: The Department of Homeland Security (DHS) serves in a leadership role by working collaboratively with, and providing support such as described below to the operational cybersecurity activities at civil agencies, State, local and tribal governments, and the private sector. This includes facilitating and contributing to national cyber risk management efforts; coordinating efforts to prepare for, protect against, and respond to cyber incidents that exceed private sector capabilities to address independently; helping to develop National cyber strategy and doctrine; developing intellectual capacity to deal with all aspects of the Homeland cybersecurity mission; contributing to research and development for that mission; sharing information with the private sector; helping to secure and defend civilian Federal networks; ensuring cross-domain situational awareness and collaboration; and continuing to address cybercrime through our existing authorities. Once it is fully operational, DHS will also be well positioned to continue broader national efforts, such as coordinating across government through the National Cyber Security Center.

The Cyber Security program in the Command, Control, and Interoperability Division supports cyber security research, development, testing, and evaluation to secure the nation's current and future critical cyber infrastructure. The Department also works through the Federal Networking and Information Technology Research and Development (NITRD) Program, with a DHS representative co-chairing the Cyber Security and Information Assurance (CSIA) Interagency Working Group, to coordinate its R&D activities across the Federal agencies and with the private sector.

The cyber environment is dynamic, and cybersecurity roles are anticipated to change in response to environmental security needs. As threats and vulnerabilities continue to evolve and emerge, DHS's role is expected to evolve accordingly.

Question#:	5
Topic:	concerns
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: Please share any concerns you have about the security of government or private computer systems that are currently not part of your department's mission or authority.

Response: Despite significant progress improving the Nation's cybersecurity posture, DHS remains concerned about the security of Federal, public- and private-sector information technology (IT) and communication systems. One of the greatest threats facing the Nation is a cyber attack against the Government or the critical infrastructure and key resources (CIKR) sectors on which the Nation depends. IT and communications support the U.S. economy and business operations and also support critical functions of government. In addition to IT and communications - for which DHS's National Cyber Security Division (NCSD) serves as the Sector Specific Agency (SSA) - DHS shares concern about attacks against major infrastructures including those supporting banking and finance; generation and distribution of energy (electricity, oil and gas); transportation; and maintenance of public water supplies. An attack could cause disruption to any or all of the CIKR sectors and could jeopardize not only the private-sector, but the Government's ability to provide critical services to the public. Such an attack could also create cascading effects throughout the country due to the integrated and global nature of business today.

61662.030

Question#:	6
Topic:	legal
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: Please describe the cyber-security measures your department is considering that are currently affected by legal restrictions.

Response: The Department of Homeland Security is coordinating with the White House as well as other departments and agencies on what potential Congressional action, including new legislation, may be needed to permit the use of cybersecurity measures that are under consideration, but potentially affected by legal restrictions.

Question#:	7
Topic:	future
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: Cyber threats to government and private systems are rapidly evolving. Are there specific concerns you have about your department's ability to perform its mission effectively in the future?

Response: For DHS to perform its mission in the future, we must create a framework that supports science and technology research for next-generation cyber security, allows for the quick insertion of new technologies and policies as well as a partnership between the public and private sectors that functions on the operational and policy levels. The funding and resources provided by the President's budget are critically important to our ability to create that framework, including specific deployment of cybersecurity tools such as the Cybersecurity Evaluation Tool and EINSTEIN. While there has been much discussion of EINSTEIN capabilities and the perimeter protection that it offers, DHS is focused on a Federal Executive Branch civilian network defense-in-depth strategy that employs perimeter defense tools with security enhancements across public sector networks and the private sector networks that support government customers. This strategy necessitates improvements to intrusion monitoring and prevention; enhanced visibility into – and assessments of – Federal Executive Branch Civilian networks; new methods to share information and improve situational awareness among cybersecurity partners; and capabilities to increase the resiliency of networks and systems. We will continue to need capabilities to monitor and prevent intrusions, technologies to assess the status of Federal systems, new methods to share and enhance information sharing on a near real-time basis, and the ability to rapidly insert new technology to counter the threats and fix vulnerabilities.

Question#:	8
Topic:	Congressional action
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: Are there areas where Congressional action may be soon be necessary to prevent dangerous vulnerabilities? If yes, please describe.

Response: The Department of Homeland Security is coordinating with the White House as well as other departments and agencies on what potential Congressional action, including new legislation, may be needed to address the evolving cybersecurity risk environment.

Question#:	9
Topic:	steps
Hearing:	Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace
Primary:	The Honorable Jon Kyl
Committee:	JUDICIARY (SENATE)

Question: Is your department taking any steps specifically to address international cyber threats to government and private systems?

Response: Yes. Threats can originate from any location and be sent to any destination, and given the international connectivity of the Internet, a significant amount of cyber attacks and crime involve an international element. Accordingly, DHS has developed and is strengthening its international capabilities. The U.S. Secret Service, for example, has extensive international liaison networks that augment and further investigations. Within the Office of Cybersecurity and Communications, the National Cyber Security Division (NCSD) builds relationships and structures to facilitate international collaboration. These relationships and structures, such as the Working Group of Key Allies[1] and the International Watch and Warning Network[2], are leveraged when needed to address threats, mitigate vulnerabilities, and manage attack consequences. In addition, NCSD tests U.S. capabilities to work with our partners in the international community through its sponsorship of the bi-annual Cyber Storm exercise, as well as other event simulations with additional international partners. DHS coordinates this work with other departments and agencies including the Departments of State and Commerce.

In addition, DHS works to address threats to government and private-sector systems in ways that help secure those systems against attack, independent of origin. The United States Computer Emergency Readiness Team (US-CERT) analyzes all threats regardless of their origin and works with its partners to identify and implement specific measures in response to identified threats, including those that emanate from overseas. Moreover, the vulnerabilities within information technology networks and systems are threat-neutral, meaning a vulnerability can be exploited just as easily by domestic or international threat actors. As a result, NCSD works with its partners to develop vulnerability mitigation strategies that are similarly threat-neutral and will reduce the likelihood of a successful cyber attack whether from international or domestic sources. These vulnerability mitigation strategies are disseminated through various mechanisms to NCSD's Federal, State, local, private sector, and international partners.

[1] The Working Group of Key Allies includes Australia, Canada, New Zealand, the United Kingdom, and the United States.
[2] The IWWN is an organization of 15 member countries composed of government cybersecurity policy makers and managers of computer security incident response teams with national responsibility.

National Security Agency Responses
to Questions for the Record from the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security Hearing,
"Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"

Responses to Questions for the Record from Senator Jon Kyl

1. While there are many aspects of cyber security, please describe the major focus of your department's involvement in the cyber security field.

NSA Response:
As mentioned in my Statement for the Record, the NSA information assurance mission focuses on protecting what National Security Directive 42 defines as "national security systems", systems that process, store, and transmit classified information or are otherwise critical to military or intelligence activities. Historically, much of our work has been sponsored by and tailored to the Department of Defense, but today national security systems are heavily dependent on commercial products and infrastructure, or interconnect with systems that are. Our strategy consists of three components:

- **Protect**: Research, develop and deploy capabilities used to secure information, and harden networks and information systems to enable mission effectiveness.
- **Defend**: Employ Information Assurance capabilities in an integrated operational environment to sense, detect, and respond to network adversaries.
- **Hunt**: Actively seek, characterize and attribute malicious activity in authorized environments to discover adversary presence and enable appropriate actions.

We also deliver IA technology, products and services meeting the operational needs of our clients; the major organizations of the Department of Defense (including the military services), the Intelligence Community and Agencies of the Federal Government.

2. What future roles is your department best suited to focus on in the cyber security field?

NSA Response:
NSA's Information Assurance Directorate has, and will continue to have, a unique and deep understanding of risks, vulnerabilities, mitigations and threats...and I believe we are recognized for this by U.S. industry, the Federal Government and our foreign partners. We have a vulnerability-discovery capability that certainly is among the best, at least among those with whom we collaborate. We can work with industry using that capability to figure out how we can make their products better and can design effective solutions. Also, we have excellent research units that will continue to be among the leading research organizations in government.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00072 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.035

3. Please share any concerns you have about the security of government or private computer systems that are currently not part of your department's mission or authority.

NSA Response:
One concern I have is that the nation is not currently at a level of security and knowledge in cyber security where we can get ahead and stay ahead of adversaries and I don't see a time in the immediate future where we'll reach the goal of consistently outmaneuvering them. In the meantime, some of America's greatest scientific, engineering and business innovations and creations...our intellectual property...is being stolen. There is not adequate recognition in industry, and in government, too, of the seriousness of the threat. It is a two-pronged lack of understanding. A lack of understanding of the threat itself and a complete lack of understanding in how to make one's business or organization a hard target. As I mentioned in my Statement for the Record, the public-private relationships are growing and thriving across the board and I think that industry will start to see cyber attacks and data theft as such a significant burden that it won't be able to be written off as a cost of doing business. Today, we're absorbing the cost of credit card fraud by having us all pay a bit more. In national security, the theft of data and disruption or interception of communications by our enemies results in much more than business losses. Defense contractors and national laboratories which are not on our secure networks have suffered targeted attacks that result in the loss of data and information critical to national security.

4. Please describe the cyber-security measures your department is considering that are currently affected by legal restrictions.

NSA Response:
NSA supports the Administration in weighing various options to improve cyber-security for the nation. Should any involve seeking legislative authority, the Administration is happy to work with the Congress.

5. Cyber threats to government and private systems are rapidly evolving. Are there specific concerns you have about your department's ability to perform its mission effectively in the future?

NSA Response:
Essentially, I'd have to answer "no." I have great confidence in our ability to perform, collaborate and improve our capabilities, as well as the capabilities of those we work with. It's certainly true that cyber threats are rapidly evolving and we have to try to stay ahead of them and outmaneuver...out-think...our adversaries. So we need to get beyond being reactive and develop methods that are proactive.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00073 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.036

6. Are there areas where Congressional action may soon be necessary to prevent dangerous vulnerabilities?

NSA Response:
We are coordinating with the White House, Office of the Director of National Intelligence, Department of Defense, and other Departments and Agencies to identify any possible Congressional actions that would help us address this evolving threat and the risk that it creates.

7. Is your department taking any steps specifically to address international cyber threats to government and private systems?

NSA Response:
As detailed elsewhere in this response, our information assurance mission is primarily focused on securing National Security Directive 42 "national security systems".

In addition, we provide standards and configuration guidance to NIST and publish information for the general public, which includes the operators of private systems. Otherwise, we do not have the authority to address the security of private systems.

The threats are global in origin and impact, so our attention is, indeed on the international cyber threats to government and private systems, and we're working with allies every day on this.

8. In your testimony you cited a variety of cyber security initiatives undertaken by NSA, but the key question is whether they resulted in NSA being more effective in countering cyber attacks. I agree with you that increased awareness of cyber security, more uniform practices, and better technology can make a difference in your department's cyber security posture, but that will only be the case if those advances outpace the advances of the attackers.

8a. Are NSA's cyber security techniques advancing faster than the expertise of cyber attackers?

NSA Response:
This is an extremely difficult question to answer, in that we don't know if we've seen the most advanced and effective techniques of our adversaries. But from what we have seen, it's a huge challenge to keep a step ahead, because the threat is constantly changing; showing up in another form or environment, originating from a different, unknown adversary, and probing or acting in a different way.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00074 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.037

8b. What percentage of cyber attacks on the systems NSA protects were thwarted in 2008 compared to 2007?

NSA Response:
The metrics on cyber attacks thwarted and vulnerabilities discovered are extremely difficult to establish with any confidence, because of the attacks that we **didn't** see or know about, and the vulnerabilities that we **didn't** find. While a decrease in the attacks we know about from year to year might indicate some level of success in protecting our networks, our focus is on the analysis of successful attacks and better ways to protect networks.

8c. How can NSA counter software that may have been left behind from prior network penetrations that can enable future attacks?

NSA Response:
This is one of our biggest concerns and that is why we established and are focusing on the HUNT component of our mission: "**actively seeking**, characterizing and attributing **malicious activity** in authorized environments **to discover adversary presence** and enable appropriate actions."

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00075 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.038

National Security Agency Responses
to Questions for the Record from the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security Hearing,
"Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"

Response to Question for the Record from Senator Orrin G. Hatch

1. Can you tell me what efforts are the NSA and NIST making in establishing measurable and auditable cyber security standards for all federal government and government contractor networks?

NSA Response:

NSA's Information Assurance Directorate (IAD) developed and distributed configuration guidance for the key components of the United States Information Technology (IT) infrastructure. Prior to September 11th, it was understood that the nation needed clear and measurable improvements in the security of critical information, and the hardening of our computers and networks to compromise. President Bush's *National Strategy to Secure Cyberspace* directed the development of a roadmap for the protection of Cyberspace. IAD's development, partnership, and security configuration guidance is an integral part of this new strategy. A key element to these activities is the NIST and IAD partnership on the development of Cyber Security Guidance Standards and Security Content Automation Protocol (SCAP), and creation of the next generation Cryptographic Standards and Recommendations. IAD is a strategic partner in developing and reviewing the NIST Special Publication in these areas.

As part of SCAP, IAD and NIST are developing standards that perform automated compliance testing with best practices benchmarked configuration and patch/vulnerability status. One of the best use cases for SCAP is providing Best Practices Benchmark Configurations and patch/vulnerability guidance in both human and machine readable formats. This enables automated assessments for both security compliance measurement and testing for the installation of critical software patches. The DoD, with NSA assistance, is implementing an enterprise-wide automated tool that can use SCAP standards to assess for compliance with mandated patches and mandated security settings (such as the Federal Desktop Core Configuration or the DoD Security Technical Implementation Guides). When these capabilities are fully deployed, the DoD will have audits of how well devices on its networks comply with relevant cyber security standards. NSA and NIST are also developing standards to fully automate reporting of compliance at local and federal levels. IAD is also partnering with Department of Energy, Department of State, and the Intelligence Community (as part of the Comprehensive National Cyber Initiative) to advocate for deployment of these SCAP-based capabilities across all federal networks.

The outcome of these efforts will be a set of standards, available commercially in commercial-off-the-shelf (COTS) products, for fully interoperable network assessment

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00076 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.039

and compliance auditing, automated remediation capabilities, and continuous machine-machine reporting of the status of security controls and security configuration items.

IAD's Center for Assured Software (CAS) leverages NIST's reporting mechanisms to publish research to help improve standards for software development across the industry. The CAS is currently working with NIST to study the capabilities of various analysis tools for programming such as C, C++, and Java. Improving these tools will enable software analysis researchers and vendors to exercise, study, and improve the capabilities of state-of-the-art tools and techniques in use today. The final goal of the effort is to enable a fully automated software assurance evaluation methodology that uses the best tools available to measure the assurance of DoD software. The team will be publishing the tests through NIST's Software Assurance Metric and Tool Evaluation (SAMATE) Reference Dataset (SRD).

IAD continuously provides technical guidance, and review of NIST publications to ensure improved standards and accurate guidance for the DoD, industry, and the Nation. NSA's unique knowledge of vulnerability and threat, coupled with a deep understanding of the operational environment provides enhanced guidance and technical input to NIST publications. Multiple communication lines are forged to support and coordinate guidance between the two organizations. NSA has forward deployed personnel at NIST focusing on international standards and identity management. We have also funded support to NIST via embedded contractors (technologists) to ensure coordination on standards and guidance across a broad spectrum of areas. Several recent publications with strong interaction between NIST and IAD include:

- SP 800-53, Rev.3 (updated September 2009):
  "Recommended Security Controls for Federal Information Systems and Organizations" - Its stated purpose is to support the "ongoing effort to produce a unified information security framework for the federal government-- including a consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls)" for the federal government and its support contractors.

- SP 800-37 (final draft, November 2009):
  "Guide for Applying the Risk Management Framework to Federal Information Systems" - Describes a revised process for certifying and accrediting federal information systems

- SP 800-117
  "The Security Content Automation Protocol (SCAP)" - Maintaining the security of information systems by automatically verifying the installation of patches, checking security configuration settings, and looking for signs of system compromise.

- Additionally, IAD provides technical support to NIST standards for cryptography, or methods for rendering plain information unintelligible to others.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00077 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.040

National Security Agency Responses
to Questions for the Record from the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security Hearing,
"Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace"

Response to Question for the Record from Senator Sheldon Whitehouse

1. Mindful of legitimate limitations on what the Executive Branch can and should disclose about sensitive cyber security initiatives, what sort of outreach, if any, have your respective agencies made to civil society groups on privacy and other civil liberties concerns? If you haven't made any such efforts yet, do you plan to? If not, why not?

NSA Response:

NSA has strongly supported this administration's policy of outreach and transparency when it comes to cybersecurity and civil liberties, and has engaged in numerous outreach efforts involving civil society groups.

NSA worked closely with the White House during the 60-day cyberspace policy review team to support a dialogue with the civil liberties and privacy community, whose views were important to the review. As a result of the review, the White House has named a privacy and civil liberties official to the new cyber security directorate. NSA is working closely with this official and with its interagency partners as part of the National Security Council's interagency policy subcommittee on privacy and civil liberties, comprised of senior privacy and civil liberties officials from a number of key agencies.

NSA is also working closely with the Department of Homeland Security (DHS) in its outreach efforts regarding the Einstein program and planned enhancements to that program. These efforts have involved significant discussion with key members of the privacy and civil liberties community, including (where clearances could be granted) at the classified level. DHS has institutionalized this outreach by forming a cyber security subcommittee for its Data Privacy and Integrity Advisory Committee, and NSA has worked closely with DHS in support of this outreach.

NSA will also receive a broad outside perspective on mission compliance and protecting civil liberties and privacy through a recently established Compliance Panel of the NSA Advisory Board. NSA reached out to a diverse, cleared group of highly-regarded experts from academia and private industry. The panel will make recommendations to NSA's senior leadership.

The American people must be confident that the power they have entrusted to NSA is not being, and will not be, abused. The intelligence oversight structure, in place now for more than a quarter of a century, is designed to ensure that the imperatives of national security are consistent with democratic values.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00078 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.041

To comply with its intelligence oversight responsibilities, NSA regularly interacts with a number of entities within the Executive Branch. These include the Intelligence Oversight Board (IOB), which reports to the President and the Attorney General on any intelligence activities the IOB believes may be unlawful. NSA also works closely with the Department of Justice, the Assistant to the Secretary of Defense (Intelligence Oversight) both NSA's general counsel and the Office of General Counsel of the Department of Defense.

Oversight and transparency – to the extent possible while protecting sources and methods – serve as needed checks on what has the potential to be an intrusive system of intelligence gathering. Directly and with its interagency partners, NSA will continue to work with outside groups, government privacy and oversight officials, and the Congress to ensure that these values will continue to guide us as we navigate the new and significant issues posed by our nation's many cyber security challenges.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00079 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.042

SUBMISSIONS FOR THE RECORD

Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SENATE JUDICIARY COMMITTEE

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

AT A HEARING ENTITLED

"CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY RIGHTS IN CYBERSPACE"

PRESENTED

NOVEMBER 17, 2009

Good afternoon, Chairman Cardin, Ranking Member Kyl, and Members of the Senate Judiciary Terrorism and Homeland Security Subcommittee. It is a pleasure to appear before you to testify about securing our nation's information infrastructure. I am pleased to share with the Subcommittee an overview of the Department of Justice's role in the U.S. Government's overall cybersecurity strategy. In light of the FBI's participation on the panel, I will limit my remarks primarily to the ways in which other components of the Justice Department address cybersecurity issues.

I. Cybersecurity Threats

As you know, information technology is embedded within and interconnects virtually all of the Nation's information and communications infrastructure, which we depend upon to conduct commercial, financial, personal, and governmental transactions. We face ongoing threats to the security of our information and information infrastructure from a wide range of actors, including nation-states, criminals, and terrorists who exploit our pervasive dependency on information technology to misappropriate or destroy information, steal money, and disrupt services, including those provided by critical infrastructures.

As recognized in the Preface to the President's *Cyberspace Policy Review*, a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity,

> [t]he architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.

Our reliance on our digital infrastructure requires that we take action to protect not only the information infrastructure itself, but also all of the data it carries and activity that it supports. The Administration is committed to integrating and organizing the government's cybersecurity efforts to better ensure that we have a comprehensive framework in place that will allow us to bring all of our tools to bear in the fight against cyber adversaries. The Department of Justice plays a key role in that fight.

II. Role of the Department of Justice

The Department works closely with our partners throughout the government – including law enforcement agencies, the Intelligence Community, the Department of Homeland Security, and the Department of Defense – to support cybersecurity efforts and inform policy discussions, as we did during the President's Cyberspace Policy Review, which was completed in May 2009. We also work closely with the National Security Council to provide legal guidance related to the unique challenges posed by threats in cyberspace, on topics ranging from the use of existing legal tools and authorities, the legality of cybersecurity programs like the EINSTEIN program, and the ways in which we can most vigorously protect privacy and civil liberties while still achieving our goal of securing the Nation's information infrastructure. With respect to the EINSTEIN program, the Department has made public two opinions from the Office of Legal

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00081 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.044

Counsel regarding that program. I will not repeat that legal analysis here but I am prepared to address any questions that members of the Subcommittee may have in that regard.

In addition, the Department has responsibility for the enforcement of laws that help secure our data and computers and for the domestic collection of foreign intelligence information, including intelligence that supports cybersecurity efforts. Through the Department's Criminal Division, especially its Computer Crime and Intellectual Property Section (CCIPS) and the U.S. Attorneys' Offices (USAOs) across the country, in coordination with our law enforcement partners at the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS), among others, we have the authority to investigate and prosecute criminal cyber actors who threaten our nation's cybersecurity. And through the Department's National Security Division (NSD), we investigate, prosecute, and prevent the cyber activities of nation-states and terrorists that pose a threat to our national security. In addition, NSD exercises oversight authority over foreign intelligence collection efforts within the United States to protect the civil liberties and privacy rights of U.S. persons.

I would like to outline briefly some of these efforts – enforcement and collection – as well as our other cybersecurity legal and policy work and our role in the protection of civil liberties and privacy.

III. Enforcement

One key part of the nation's overall cybersecurity effort is the investigation and prosecution of cyber criminals – with the goal of incapacitating or deterring them before they can complete an attack on our networks, or punishing them and deterring similar future acts if there is a successful intrusion.

The Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cyber crime wherever it occurs. A nationwide network of over 230 Computer Hacking and Intellectual Property (CHIP) prosecutors in our USAOs focuses on these crimes, coordinated through the Criminal Division's CCIPS. These prosecutors, as well as all prosecutors working cybercrime cases throughout the country, work closely with all of our law enforcement partners, including the FBI, the USSS, and the U.S. Postal Inspection Service. In addition, we have a strong partnership with the National Cyber Investigative Joint Task Force, which brings together law enforcement, intelligence, and defense agencies to focus on high-priority cyber threats.

Litigating components of the Department's NSD -- the Counterespionage and the Counterterrorism Sections -- share the Criminal Division's responsibility for safeguarding the country's information systems through enforcement of criminal laws. The Counterespionage Section prosecutes misappropriation of intellectual property to benefit a foreign government, as provided by the Economic Espionage Act of 1996 (18 U.S.C. § 1831), and obtaining national defense, foreign relations, or restricted data by accessing a computer without authorization, as provided by section 1030(a)(1) of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The Counterterrorism Section – leveraging the capabilities and expertise of CCIPS, CHIP prosecutors, the Anti-Terrorism Advisory Council, and Joint Terrorism Task Forces – would

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00082 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.045

play a pivotal role in addressing any major cybersecurity attack by terrorists or associated groups or individuals.

A. Operational Successes

The relationships between the Department's prosecuting components and the federal investigative agencies, and the robust cooperation and information sharing that they support, have led to a number of enforcement successes – just a few of which I would like to highlight here.

- **Phish Phry.** Last month, nearly 100 people were charged in the U.S. and Egypt as part of an operation known as Phish Phry – one of the largest cyber fraud phishing cases to date. "Phishing" is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Phish Phry was the latest action in what Director Mueller described as a "cyber arms race" where law enforcement must coordinate and collaborate in order to keep up with its cyber adversaries. The defendants in Operation Phish Phry targeted U.S. banks and victimized hundreds of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled. More than 50 individuals in California, Nevada, and North Carolina, and nearly 50 Egyptian citizens have been charged with crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identify theft. This investigation, led by the FBI, required close coordination with the USSS, the Electronic Crimes Task Force, the USAO in the Central District of California, state and local law enforcement, and our Egyptian counterparts. In fact, Phish Phry represents the first joint cyber investigation between Egypt and the United States.

- **RBS WorldPay.** Just last week, as a result of unprecedented international law enforcement cooperation, four members of an alleged international hacking ring were indicted in Atlanta for their participation in a highly sophisticated and organized computer fraud attack. They face various charges related to allegedly hacking into a computer network operated by the Atlanta-based credit card processing company RBS WorldPay, which is part of the Royal Bank of Scotland. Sergei Tsurikov of Estonia, Viktor Pleshchuk of Russia, Oleg Covelin of Moldova, and a person known only as "Hacker 3" allegedly used sophisticated hacking techniques to compromise the data encryption that RBS WorldPay used to protect customer data on payroll debit cards, which enable employees to withdraw their regular salaries from an ATM. Once the encryption on the card processing system was compromised, the hacking ring allegedly raised the account limits on compromised accounts and then provided a network of "cashers" with 44 counterfeit payroll debit cards, which were used to withdraw more than $9 million from more than 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. The $9 million loss occurred within a span of less than 12 hours. Four other individuals from Estonia were also charged in Atlanta with access device fraud for their involvement in the scheme. This investigation, led by the FBI,

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00083 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.046

required close coordination not only with other domestic law enforcement partners, including the USSS, the USAO in Atlanta, and various components of the Department's Criminal Division, including CCIPS and the Office of International Affairs, but also with numerous international partners, including the Estonian Central Criminal Police and the Estonian Office of the Prosecutor General, the Hong Kong Police Force, and the Netherlands Police Agency National Crime Squad High Tech Crime Unit and National Public Prosecutor's Office.

- **International hacking ring.** In September 2009, Albert Gonzalez, a hacker involved in one of the largest hacking and identity theft case ever prosecuted, pleaded guilty to 20 counts of conspiracy, computer fraud, wire fraud, access device fraud, and aggravated identity theft in the District of Massachusetts and the Eastern District of New York. Gonzalez was part of an international hacking ring responsible for the theft of more than 40 million credit and debit card numbers from various retailers, including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave & Buster's, and DSW. In all, 11 ring members from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus were indicted in this case. Gonzalez remains under indictment in the District of New Jersey on charges related to a conspiracy to hack into computer networks supporting major U.S. retail and financial organizations, including Heartland Payment Systems and 7-Eleven, and steal credit and debit card numbers from those entities. Another defendant in this case, Maksym Yastremskiy, known online as "Maksik," was ultimately arrested for his carding activity in Turkey, and earlier this year, was sentenced by a Turkish court to 30 years in prison. Maksik is believed to be one of the top traffickers in stolen account information.

- **DarkMarket carding forum**. On October 16, 2008, the FBI announced the results of a two-year undercover operation, conducted in conjunction with CCIPS, targeting members of the online carding forum known as DarkMarket. At its peak, the DarkMarket website had over 2,500 registered members around the world. This operation, which required unprecedented international cooperation, involved law enforcement from countries ranging from Ukraine to Turkey to Romania to France. It resulted in approximately 60 arrests worldwide and prevented an estimated $70 million in economic loss.

- **"Hacker Havens."** A number of recent investigations begun in the U.S. have resulted in successful prosecutions in several foreign countries long considered to be so-called "hacker havens." As just one example, based on close cooperation between the Department, the FBI, and the Romanian National Police Cybercrime Divisions, prosecutors from Romania's Directorate for Investigating Organized Crime and Terrorism arrested 11 Romanian citizens on fraud and identity theft charges in November 2007. They were part of a criminal organization that specialized in "phishing" information from computer users, imprinting credit and debit card information onto counterfeit cards, and then using those cards to obtain cash from ATMs and Western Union locations. Romanian police officers executed 21 search warrants and seized computers, card reading and writing devices, blank cards, and

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00084 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.047

other equipment. More recently, between February 2008 and March 2009, over 40 defendants were charged in Romania – along with 12 in the United States – for their participation in a sophisticated hacking scheme involving the theft of corporate bank account information, and the use of that stolen information in a variety of fraudulent transactions.

- **Economic Espionage.** In June 2008, Xiaodong Sheldon Meng, a software engineer born in China, received the first sentence handed down by a federal court for a violation of the Economic Espionage Act for misappropriating intellectual property to benefit a foreign nation. He also was sentenced for violating the Arms Export Control Act and the International Traffic in Arms Regulations. Meng's conviction involved the theft of source code known as "Mantis 1.5.5" (simulator technology used for military training and other purposes) from his former employer, Quantum3D Inc., with the intent to benefit the People's Republic of China (PRC) Navy Research Center in Beijing.

It is important to understand that one of the key challenges that we face in pursuing cyber criminals is to accurately attribute the source of an intrusion. Often we cannot easily tell who is perpetrating these actions – a nation-state, a terrorist, or a criminal individual or group – but regardless of the actor, the effect is often the same. These kinds of cyber intrusions undermine the Nation's economic and national security, and the Department is committed to enforcing the laws designed to prohibit these incidents.

B. Capacity Building and Legal Tools

Beyond our own operational successes, the Department also engages in extensive capacity building through training programs, both domestic and international, that augment the U.S. Government's ability to investigate and prosecute cyber incidents. Every year, we train hundreds of domestic law enforcement agents on the legal tools we use in our enforcement efforts. These legal tools include substantive criminal laws that establish criminal conduct, such as the Computer Fraud and Abuse Act (18 U.S.C. § 1030), but also the laws that empower us to gather evidence to investigate such conduct, such as the Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.). The penalties for hacking crimes could be enhanced to better deter criminals, and a law requiring data breach reports to federal law enforcement would help us better investigate and prosecute large-scale security breaches. The Department stands ready to work with Congress to this end.

In addition, we engage extensively with our foreign law enforcement partners. Only by assisting foreign authorities can we expect them to reciprocate with vital evidence for our own investigations. As such, we often begin domestic investigations that lead to successful foreign prosecutions, as in the hacker haven cases I discussed above. And even purely domestic investigations often rely on evidence from overseas, such as where a U.S. hacker routes his communications through foreign computers before attacking a U.S. victim. CCIPS also is the United States Point of Contact in the G8 High-Tech Crime's 24/7 network, which consists of 55 member countries and is designed to connect international law enforcement partners with each other at any time to facilitate investigative cooperation.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00085 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.048

Beyond this kind of assistance, we also train foreign law enforcement agencies each year on electronic evidence collection and international cooperation, and we provide technical and drafting assistance for countries developing laws criminalizing malicious cyber activity. To promote foreign legal development, we believe that the United States should continue to press other nations to accede to the Convention on Cybercrime (2001). Broader membership in the Convention will improve cooperation between law enforcement agencies by creating consistent substantive laws, and by improving procedural laws across the globe to facilitate the United States' ability to quickly and easily get foreign evidence required for a domestic investigation.

IV. Foreign Intelligence Collection and Oversight

The Department also supports the Intelligence Community's cybersecurity efforts through the work of NSD's Office of Intelligence. The Office of Intelligence plays a pivotal role in many facets of the Intelligence Community's efforts to protect the nation, including its burgeoning cybersecurity efforts. In particular, the Office of Intelligence represents the U.S. Government before the Foreign Intelligence Surveillance Court to obtain the authority for the FBI and other members of the Intelligence Community to collect foreign intelligence pursuant to the Foreign Intelligence Surveillance Act, as amended (50 U.S.C. § 1801, et seq.) (FISA). Because almost all activity conducted pursuant to FISA is classified, I am limited in what I can say in this hearing about the Department's cybersecurity activities under that statute. However, I would be happy to provide you with more information about such activities in an appropriate forum.

It is important for me to emphasize that in addition to providing support to the Intelligence Community's cybersecurity activities—as well as its other intelligence gathering responsibilities conducted domestically or involving U.S. persons abroad—the Department also has significant responsibilities for protecting civil liberties. While the Department has increased its efficiency in preparing and submitting FISA applications to the FISC, it also has enhanced its ability to ensure that these applications furnish all of the privacy protections provided by the FISA statute. Moreover, the Department has assumed increased responsibility for ensuring that the intelligence and counterintelligence activities of the FBI, as well as those of other intelligence agencies, adhere to the Constitution and applicable laws of the United States. Through activities such as the review and approval of guidelines as provided by Executive Order 12333 governing Intelligence Community activities, the Department plays a central role in safeguarding vital civil liberties as we help protect the Nation.

V. Other Cybersecurity Efforts

Finally, the Department plays a key role in the policy development process and the implementation of technical cybersecurity measures. The Department's Criminal Division, NSD, and Chief Information Officer's Office, have been heavily involved in interagency policy development on issues related to incident response, information sharing, technical architecture, coordinating cyber operations, international engagement, and public awareness.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00086 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.049

The Department's Chief Information Officer (CIO) has also strengthened the Department's network defenses by reducing the number of Internet connections to consolidate traffic, providing in-depth monitoring of those connections and supporting security upgrades to gateway services. In addition, the Department CIO has recently invested in an enterprise tool that will provide real time situational awareness of network operations, monitor secure configuration controls and streamline patch management. The Department's Justice Security Operations Center (JSOC) analyzes EINSTEIN 1 data to support its mission of defending Department computer networks. While JSOC possesses more robust network traffic tools, the EINSTEIN 1 appliance provides an efficient mechanism to query network traffic flows in support of computer security incident response.

In addition to our policy work, the Department also plays a unique role in providing legal guidance on issues related to cybersecurity. Working in coordination with Offices of General Counsel throughout the U.S. Government, we have analyzed the EINSTEIN program, with which you are familiar, and taken steps to ensure that our cybersecurity efforts not only rest on sound legal footing but also vigorously protect civil liberties and privacy.

VI. Existing Legal Authorities and Civil Liberties Protections

One of the Department's responsibilities is to ensure that it is using existing legal authorities to the fullest extent possible, and to continually review those authorities to make sure that they are effective in addressing today's challenges. The law applicable to cyber-security activities is very complex and difficult to summarize succinctly. That domestic and international legal regime necessarily defines and limits available policy options, and impacts the relationship between the government and the private sector on cyber issues. As set forth in the Administration's *Cyberspace Policy Review*:

> Law applicable to information and communications networks is a complex patchwork of Constitutional, domestic, foreign, and international laws that shapes viable policy options. In the United States, this patchwork exists because, throughout the evolution of the information and communications infrastructure, the Federal government enacted laws and policies to govern aspects of what were very diverse industries and technologies.
>
> As traditional telecommunications and Internet-type networks continue to converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity, law and policy should continue to seek an integrated approach that combines the benefits of flexibility and diversity of applications and services with the protection of civil liberties, privacy rights, public safety, and national and economic security interests . . . . Policy decisions will necessarily be shaped and bounded by the legal framework in which they are made, and policy consideration may help identify gaps and challenges in current laws and inform necessary developments in the law. That process may prompt proposals for a new legislative framework to rationalize the patchwork of overlapping laws that apply to information, telecommunications, networks, and technologies, or the application of new interpretations of existing laws in ways to meet technological evolution and policy goals, consistent with U.S. Constitutional principles. However, pursuing either

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00087 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.050

course risks outcomes that may make certain activities conducted by the Federal government to protect information and communications infrastructure more difficult.

The Department looks forward to continuing to work with Congress to better ensure that our laws address properly the threats and challenges that all of us – including the government, the private sector, and the public – face today and provide for appropriately robust law enforcement, intelligence, and other cyber-related authorities, consistent with civil liberties and privacy protections. As noted above, any changes we make must be well-considered to reduce the likelihood that they will have unintended consequences that adversely impact law enforcement or intelligence activities or privacy rights.

VII. Conclusion

I would like to thank the Subcommittee for the opportunity to share with you, and the American people, the high priority the Department places on cybersecurity and the work we do to protect the Nation's information and communications infrastructure through cyberspace policy development, law enforcement, and intelligence collection. We recognize that each of the federal components testifying here today plays a distinct and vital role in cybersecurity, and we look forward to continuing to work with them and all of our partners throughout the government, in the private sector, and across the globe, to achieve our common goal of assuring a trusted and resilient information and communications infrastructure.

This concludes my remarks. I would be pleased to answer questions from you and other members of the Subcommittee.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00088 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.051

Statement of

The Honorable Benjamin L. Cardin

United States Senator
Maryland
November 17, 2009

OPENING STATEMENT OF

SENATOR BENJAMIN L. CARDIN

CHAIRMAN, TERRORISM AND HOMELAND SECURITY SUBCOMMITTEE

OF THE SENATE JUDICIARY COMMITTEE

HEARING: "CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE

Tuesday, November 17, 2009

The subcommittee will come to order.

Today the subcommittee examines one of the most important subjects – and frankly one of the most complicated subjects – that Congress and the Obama Administration must address in the coming months, and that is cybersecurity. Today hearing is entitled "Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace."

The internet was initially designed as a research tool for the sharing of information, and today has grown into one of the most remarkable innovations of the technological and information revolution. The internet has greatly expanded the dissemination of information to individuals across the planet, and has allowed for a greater and more robust exchange of ideas in our new digital global marketplace.

With these improvements comes many new dangers, however. Today Senators will hear testimony that describes a range of new technological challenges that threaten to undermine cybersecurity and the ability of governments, citizens, and the private sector to safely and securely use the internet. Today we will have a bit of an education for Senators about some new technological terms in cybersecurity, including botnets, targeted and blended phishing, spyware, and malware. Our current system allows criminals, hackers, and terrorists to exploiting the weaknesses of the internet to gain access to confidential and classified information. Such attacks could also manipulate, corrupt, or alter data that is being used to run critical information systems inside the government or private businesses.

Soon after taking office, President Obama ordered a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity. The review team of government cybersecurity experts engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches. In May 2009, the CyberSpace Policy Review ("Review") summarized the review team's conclusions and outlined near-term and mid-term action items, for moving toward a reliable, resilient, and trustworthy digital infrastructure for the future.

This Review contained some sobering conclusions.

The Review stated that "the federal government is not organized to address this growing problem effectively now or in the future. Responsibilities for cybersecurity are distributed across a wide array of federal departments and agencies, many with overlapping authorities, and none with sufficient decision authority to direct actions that deal with often conflicting issues in a consistent way."
The executive summary concludes that "the nation is at a crossroads?the status quo is no longer acceptable?the national dialogue on cybersecurity must begin today?"

It also stated that "the United States cannot succeed in securing cyberspace if it works in isolation?the Federal government cannot entirely delegate or abrogate its role in secure the Nation from a cyber incident or accident?working with the private sector, performance and security objectives must be defined for the next-generation infrastructure?"

Finally, the report states that "the White House must lead the way forward."

Today's hearing will therefore examine both governmental and private sector efforts to prevent a terrorist cyberattack, which if successful could cripple large sectors of our government, economy, and essential services. I note that the first recommendation from the Review was to "appoint a cybersecurity policy official responsible for coordination the Nation's cybersecurity policies and activities."

The hearing will also examine the proper balance between improving cybersecurity and protecting the privacy rights and civil liberties of Americans.

I note that another recommendation from the Review was to "designate a privacy and civil liberties official to the NSC cybersecurity directorate."

Finally, we will examine the proper role of government in setting standards for the private sector or taking control of the internet or computer systems in an emergency.

I look forward to the testimony of our distinguished panel of government witnesses on Panel 1, including the Department of Justice, Department of Homeland Security, National Security Agency, and the Federal Bureau of Investigation.

I also look forward to the testimony of our distinguished panel of outside witnesses on Panel 2, including the Center for Democracy and Technology, the Internet Security Alliance, and the U.S.-China Economic and Security Review Commission.

I will now recognize Senator Kyl, the Ranking Member of our Subcommittee, for any remarks that he would care to make at this time.

Department of Justice

STATEMENT OF

STEVEN R. CHABINSKY
DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SENATE JUDICIARY COMMITTEE

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

AT A HEARING ENTITLED

"CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY RIGHTS IN CYBERSPACE"

PRESENTED

NOVEMBER 17, 2009

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00092 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.055

Good morning Chairman Cardin, Ranking Member Kyl, and distinguished members of the subcommittee. I am pleased to be here today to discuss the Federal Bureau of Investigation's role in reducing our nation's risk from acts of cyber terrorism, cyber espionage, and cyber crime.

The Cyber Threat and the FBI's Cyber Program

The FBI considers the cyber threat against our nation to be one of the greatest concerns of the 21st century. Despite the enormous advantages of the Internet, our networked systems have a gaping and widening hole in the security posture of both our private sector and government systems. An increasing array of sophisticated state and non-state actors have the capability to steal, alter, or destroy our sensitive data and, in the worst of cases, to manipulate from afar the process control systems that are meant to ensure the proper functioning of portions of our critical infrastructure. Moreover, the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes continues to rise.

When assessing the extent of the cyber threat, the FBI considers both the sophistication and the intent of our adversaries. The most sophisticated actors have the ability to alter our hardware and software along the global supply chain route, conduct remote intrusions into our networks, establish the physical and technical presence necessary to re-route and monitor our wireless communications, and plant dangerous insiders within our private sector and government organizations. The actors that currently have all of these capabilities -- which is a finding that is distinct from whether and when they are using them -- include multiple nation states and likely include some organized crime groups.

In the cyber realm, the technical positioning an adversary requires to steal data typically provides them with the very same access and systems administrator rights that could be used for destructive purposes. As a result, Computer Network Exploitation -- the ability of foreign spies to monitor our networks and steal our secrets -- might simultaneously provide our enemies with pre-positioned capabilities to conduct Computer Network Attack -- the ability to deny, disrupt, degrade, or destroy our information, our networks, and the infrastructure services that rely upon them.

With respect to organized crime groups, financially motivated cyber crime typically does not involve acts of violence or network destruction. The exception to this generality however is extortion. Cyber criminals can threaten to hold entire networks, or more simply the data on them, hostage to their demands. Often, cyber criminals have the technical sophistication and access to make good on their threats, especially if an insider is involved.

The FBI has not yet seen a high level of end-to-end cyber sophistication within terrorist organizations. Still, the FBI is aware of and investigating individuals who are affiliated with or sympathetic to al-Qaeda who have recognized and discussed the vulnerabilities of the U.S. infrastructure to cyber attack, who have demonstrated an interest in elevating

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00093 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.056

their computer hacking skills, and who are seeking more sophisticated capabilities from outside of their close-knit circles. Should terrorists obtain such capabilities, they will be matched with destructive and deadly intent. In addition, it is always worth remaining mindful that terrorists do not require long term, persistent network access to accomplish some or all of their goals. Rather, a compelling act of terror in cyberspace could take advantage of a limited window of opportunity to access and then destroy portions of our networked infrastructure. The likelihood that such an opportunity will present itself to terrorists is increased by the fact that we, as a nation, continue to deploy new technologies without having in place sufficient hardware or software assurance schemes, or sufficient security processes that extend through the entire lifecycle of our networks.

FBI Leadership, Collaboration, and Information Sharing

Based on the significance of the problem, protecting the United States against cyber-based attacks and high-technology crimes is one of the FBI's highest priorities and, in fact, is the FBI's highest criminal priority. It is with these factors in mind that, in 2002, the FBI created its current Cyber Division to handle all categories of cyber crime and cyber national security matters.

Today's FBI is comprised of the largest cadre of cyber trained law enforcement officers in the United States, with over 2,000 Special Agents having received specialized cyber training as part of the core curriculum at Quantico. To combat the most sophisticated and urgent matters, the FBI has built a national resource of over 1,000 advanced cyber-trained FBI Special Agents, Intelligence Analysts, and Digital Forensic Examiners. In short, some of the best and brightest minds in the country have joined the FBI, which is positioned with the statutory authority, expertise, and ability to mitigate, disrupt, prevent, and investigate illegal computer-supported operations domestically.

Still, the cyber threat will not be eliminated through the efforts of any one government agency acting alone. It is for this reason that we have made collaboration and information sharing a key component of the FBI cyber strategy. The FBI has established a leadership role across the federal government, with industry, with state and local partners, with consumers, and internationally.

At the federal level, the FBI established and leads the National Cyber Investigative Joint Task Force, a Presidentially mandated focal point for all government agencies to coordinate, integrate, and share pertinent information related to all domestic cyber threat investigations.

Serving by example, the FBI also leads all law enforcement agencies in cyber information sharing. In Fiscal Year 2009, the FBI disseminated over 1,800 cyber intelligence reports and cyber analytic products, providing members of the Intelligence Community, military, and Department of Homeland Security with the information they need to maximize their and our nation's success.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00094 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.057

At the industry, state, and local level, the FBI established and leads InfraGard, currently consisting of more than 33,000 members spanning 87 cities nationwide and including representatives from federal, state, and local government, industry, and academia. InfraGard is the nation's largest government/private sector partnership focused on reducing physical and cyber threats against our critical infrastructure. Although InfraGard is an FBI program, established in 1996, it also benefits from the active support and participation of the Department of Homeland Security and each of its Protective Security Advisors throughout the country. The FBI also established a lead role in the development of the National Cyber Forensics and Training Alliance, a group committed to combining the resources of academia, law enforcement, and industry to identify major global cyber threats.

At the consumer level, the FBI established and leads the Internet Crime Complaint Center (IC3) in partnership with the National White Collar Crime Center. The IC3 website (www.ic3.gov) is the leading cyber crime incident reporting portal, having received 275,284 complaint submissions in 2008 alone. From these submissions, IC3 analyzed, aggregated, and then referred 72,940 complaints of crime to federal, state, and local law enforcement agencies around the country for further consideration.

Internationally, the FBI operates 75 Legal Attache offices and sub-offices around the world to assist in international investigations, including cyber investigations, providing coverage for more than 200 countries, territories, and islands. The FBI's international efforts have led to the arrest of hundreds of cyber criminals throughout the world, resulting in the dismantlement of major transnational organized crime rings that once preyed on Americans. The FBI also plays a leading role in the National Intellectual Property Rights (IPR) Center which, together with U.S. Immigration and Customs Enforcement and U.S. Customs and Border Protection, coordinates the government's domestic and international law enforcement efforts against IPR violations.

FBI Investigative, Collaborative, and Information Sharing Success

Although an unclassified forum is not suitable for discussing the FBI's counter-terrorism and counter-intelligence cyber efforts, our investigative success on the criminal side provides a glimpse into our capabilities and strategic partnerships that can be used against any adversary. These cases also serve as a warning to would-be cyber thieves: the FBI can and will investigate high technology crimes, we have partners throughout the world who are equally capable and vigilant, and we will ensure that cyber criminals are brought to justice.

Take for example last year's RBS Worldpay case in which a transnational crime organization used sophisticated hacking techniques to withdraw, in less than 12 hours, over $9 million from 2,100 ATM machines in 280 cities around the world, including the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. The FBI led the investigation, and its work with international law enforcement led to multiple arrests throughout the world, and last week's indictment by a federal grand jury in Atlanta. The FBI investigation also included United States Secret Service participation,

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00095 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.058

providing them with information that was relevant to their investigation of intrusions into Heartland Payment Systems and TJX Companies, for which there was a separate indictment in August of 2008. Each of these cases also included strong law enforcement assistance from the victims, which proved invaluable. Simply put, working together works.

The FBI's Operation Phish Phry is another recent example of the successful relationships between the FBI, the private sector, and international partners. Phish Phry resulted from ongoing coordination efforts between the FBI and United States financial institutions. Through the course of a two year investigation, the investigation uncovered thousands of victims and identified an international sophisticated computer intrusion, identity theft and money laundering scheme comprised of hundreds of subjects in the United States and Egypt. The FBI investigation yielded a 51 count Federal indictment charging 53 U.S. citizens, while Egyptian law enforcement identified 47 Egyptian suspects directly involved in the criminal conspiracy. Of the identified U.S. targets, 10 possessed violent criminal histories requiring FBI SWAT teams to execute the high risk arrests. Cybercrime is serious business, and the people involved in it are no longer 15 year olds in their parents' homes. Cybercrime is increasingly being adopted as a profitable component of violent, organized, sophisticated, well-financed crime rings.

Another case example of note is the FBI's infiltration and dismantlement of Darkmarket, an online virtual transnational criminal organization. Working with our international partners in the United Kingdom, Germany, and Turkey the FBI conducted a two year undercover operation to penetrate the organization and bring it to its knees. At its peak, the Darkmarket forum had over 2,500 members, spanning countries throughout the world, who were involved in buying and selling stolen financial information, including credit card data, login credentials (user names, passwords), and equipment used to carry out certain financial crimes. Using undercover techniques, the FBI penetrated the highest levels of this group and identified and located its leading members. Multi-agency and multi-national coordination with our law enforcement partners led to over 60 arrests worldwide, as well as the prevention of $70 million in economic loss that otherwise would have occurred from compromised victim accounts.

In order to better protect banks and consumers against the rising costs of online fraud, the FBI has ramped up its collaboration to address matters impacting the financial services industry. In December of 2008, the FBI -- working with the Internet Crime Complaint Center -- issued a press release titled "Web Site Attack Preventative Measures" identifying a considerable spike in cyber attacks against the financial services and the online retail industry, and detailing a number of actions a firm can take in order to prevent or thwart the specific attacks and techniques used by the intruders we were monitoring. This year, the FBI and the Financial Services Information Sharing and Analysis Center (FS-ISAC) developed a new model for intelligence driven collaboration between law enforcement and the private sector. Specifically, during the course of our investigations, the FBI recognized threat trends, tactics, and techniques involving Automated Clearing House (ACH) transactions. Not only did we share that information while our investigations were pending, we invited FS-ISAC representatives into FBI

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00096 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.059

space to get a full briefing on our case information. We then asked the FS-ISAC whether the threat information the FBI was seeing was relevant and timely for businesses and consumers to use to better protect themselves, reduce their vulnerabilities, and mitigate the consequences of these types of fraud. Industry representatives not only agreed that the information was pertinent, but that a written product would be useful for its members. In an entirely new collaboration model, we created a joint product in which the FBI wrote the first two sections involving the nature of the threat and how to recognize it, and the FS-ISAC (working with the National Automated Clearing House Association) wrote the second two sections involving industry impact and security recommendations for preventing further fraud.

Each of the above examples demonstrate that he FBI has not only adopted a robust information sharing model, we have moved past it. Our experience shows that collaboration is the answer, with information sharing being only one component of the equation. Taking advantage of each partner's skills and knowledge, and leveraging our nation's combined strengths in common cause, provides significant advantages that are leading to increased and repeatable successes. Which brings me to the FBI's way ahead.

The Way Ahead

In an era of ever growing adversaries, our success clearly depends on working together and ensuring that agencies and industry have mature models in place for sharing information and collaborating, and to do so fully consistent with all civil liberties and privacy protections. Only in this way can we deter our adversaries, locate and bring them to justice, minimize systems vulnerabilities, and ensure that the consequences of successful cyber breaches and attacks are reduced.

As I alluded to earlier, the Federal government's designated hub for domestic cyber threat investigative coordination, integration, and information sharing is the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF is a central aspect of the FBI's -- and the nation's -- comprehensive strategy to investigate, predict, and prevent cyber terrorism, cyber espionage, and cyber crime. In this regard, I would like to acknowledge the 19 intelligence and law enforcement agencies who, in addition to the FBI, have representatives at the NCIJTF and who are making vital contributions to our nation's cyber security every day.

Conclusion

I am grateful to the subcommittee for this chance to highlight the FBI's strengths in combating terrorism, espionage, and crime in cyberspace, and to recognize the partnerships that allow us to meet this ever growing economic and national security problem. I am happy to answer any questions you may have.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00097 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.060

TESTIMONY OF LARRY CLINTON,
PRESIDENT AND CEO OF THE INTERNET SECURITY ALLIANCE

UNITED STATES SENATE JUDICIARY COMMITTEE
NOVEMBER 17, 2009

Good morning. I am Larry Clinton, President of the Internet Security Alliance (ISA). I want to thank the Judiciary Committee for inviting me to testify today.

ISA was born in 2001, in collaboration with Carnegie Mellon University, as a trade association of major business users of internet security services. ISA is organized like the internet. We are international in our membership, with members on 4 continents, and we are cross-sectored in our representation. ISA represents members of the banking, insurance, defense, manufacturing, business integration, information technology, and telecommunications industries.

The ISA mission is to integrate advanced technology with both the pragmatic business imperatives of the owners and operators of the Internet - namely the private sector - and enlightened public policy to create a sustainable system of cyber security.

In November of 2008, the ISA published its policy recommendations for the 111th Congress and the Obama Administration: the Cyber Security Social Contract. Through this document we argued that, in the last century, when the hot new technology was phones and electricity, policy makers wisely realized that there was a public interest in universal phone and electric service and that universal service would not be achieved unless the government used its economic powers to intervene.

As a result, the government made a deal, a social contract, with the private sector providers of these services that essentially guaranteed the return on their private investment if that investment would service the public policy goal of universal service. That particular use of market incentives for private infrastructure investment worked, and it provided the basis for a century of American industrial and military prominence.

We have a similar situation today, in the fact that we need universal cyber security. Due to the interconnectedness of the system, one entity's insecurity

61662.061

can cause tremendous harm to others downstream, including the government and the nation as a whole. Government will need to motivate private investment in infrastructure upgrades to serve this national interest.

ISA was delighted when President Obama came out with his Cyber Space Policy Review in May of 2008 especially because the first item quoted in that document was the ISA Cyber Security Social Contract.

In fact, the Executive Summary to the Administration's document both begins and ends by citing ISA documents, and the Cyber Space Policy Review goes on to cite more than a dozen other ISA white papers and submissions---far more citations than from any other source.

Naturally, ISA supports the Administration's Cyber Space Policy Review for a wide variety of reasons.

First, the President is correct in his appreciation of the need to view cyber security as not just a technical and security issue, but as an economic one as well. Notwithstanding the delay in appointing a cyber coordinator, we believe that it is absolutely correct to design that position with a line of authority to the National Economic Council, as well as the National Security Council.

In the 21st century - the digital century - economics and security are opposite sides of the same coin. You cannot affect one without impacting the other.

Second, in his White House speech on cyber security, the President was absolutely correct when he said he was opposed to regulatory, mandated standards on the private sector for cyber security. Federally-imposed mandates on the broad private sector will not work and will be seriously counterproductive to both our economic security and our national security.

Third, the Administration's Cyber Space Policy Review takes the right approach in advocating for the development of additional economic incentives, including procurement incentives, liability incentives, and even tax incentives, to promote cyber security. This approach is in line with the precedent set for successful infrastructure upgrades via the social contract that government struck with industry a century ago, as well as with the model for cyber security that ISA laid out last November, and it is the most

pragmatic path to achieving the critical national security goals that are government's priority.

There are many particulars in the Administration's document that the ISA also supports. In fact, on December 3, we will be releasing a new publication entitled, "Implementing the Obama Cyber Security Strategy via the Social Contract Model." This new document will detail specific steps to move from broad policy principles, where we find broad agreement, to implementation, and it will cover issues such as:

- Securing the global IT supply chain
- Developing a new information sharing model generating actionable information for the broad range of the private sector
- Aligning and managing the legal incongruities created by modern technologies and outdated legal structures
- Creating both a market and incentives to promote proven effective cyber security standards/practices and technologies
- Creating an enterprise education program to enable modern corporations to properly appreciate and manage financial cyber risk
- Addressing the critical cyber security issues facing higher education
- Developing automated security standards for unified communications platforms such as VOIP

However, given the short amount of time that I have with the Senate Judiciary Committee, I will focus my oral comments on three major truths that I believe to be central for Congress to understand if it is going to legislate on the issue of cyber security.

These are:

I. The Internet changes everything
II. Cyber security is as much an economic issue an "IT" issue
III. We will need to develop new understandings about government and industry's roles and responsibilities, and limitations if we are to address this serious 21st century problem on a sustainable basis.

I. THE INTERNET CHANGES EVERYTHING

Most of us in this room are part of the group that demographers are now calling the "digital immigrants," meaning that we, unlike my teenage children who are 'digital natives," were not born into this digital world we that now surrounds us.

While senior policy makers, such as the members of this committee, can successfully adapt to their new digital world, it is important for them not to simply assume that the assumptions and governance models developed primarily during the cold war era apply well to digital technology.

The Internet is the quintessential example of this phenomenon. The Internet is unlike anything we have dealt with before. Consequently, it will require a security system unlike anything we have designed before.

How, then, is the Internet different?

- It transmits phone calls, but it is not a phone line.
- It makes copies, but it is not a Xerox machine.
- It houses books, but it is not a library.
- It broadcasts images, but it is not a TV station.
- It's critical to our national defense, but it is not a military installation.
- It's all these things, and much more.

The Internet is international, interactive, constantly changing, constantly under attack, and then it changes again.

It's not even really an "It." It's actually lots of "Its" all knitted together. Some 'Its' are public, some are private, but all transmit information across corporate and national borders without once stopping to pay tolls or to check regional sensitivities.

We can not simply "cut and paste" previous governance systems from old technologies or business models and realistically expect that we will be able to manage this new system effectively.

The regulatory model that we have traditionally used to govern business has not changed much since we created it to deal with the breakthrough technology of 2 centuries ago - the railroad.

61662.064

To manage the railroad, Congress decided to create an expert agency, the ICC, to pass specific regulations. The ICC begat the rest of the alphabet soup regulatory agencies: the FCC, the SEC, the FTC. That system, for the most part, has worked arguably well.

However, that system will not work with Internet security. Even if Congress were to enact an enlightened statute, it would not have reach beyond our national borders and, hence, it would not be comprehensive enough. Even if some agency wrote a brilliant regulation, that regulation is likely to be out-dated before it got through the process, a process that can be further delayed through court challenges.

This also assumes, unrealistically, that the political process inherent in a government regulation system doesn't "dumb-down" the eventual regulations so that we wind up with a campaign finance-style standard, where everyone can attest that they are meeting the federal regulations, but everyone knows that the system is not really working.

That approach might work in politics, but, frankly, we can't afford it when it comes to Internet security.

Yet, we can't stand idly by, either. Together we must develop a mechanism to assure an effective and sustainable system of security that will accommodate the global breadth of the Internet and yet still result in a dynamic and constantly improving system of mutual security.

We, the Internet Security Alliance, contend that the best mechanism to assure an adequate and sustainable defense system is to inject the market. We need to have corporations, who own and operate the vast majority of the Internet, to perceive that it is in their own self interest to continually improve not only their own security, but also the security of everyone else with which they interact. In order for us to create such a system, we need to appreciate the second core truth, namely:

II. Cyber Security is as much an Economic issue as an "IT" issue.

Until just recently, it was common for information security policy discussions in Washington to take place without any reference to economic issues. However, corporate suites are one arena in which these discussions rarely ignore economics.

As PricewaterhouseCoopers' 2009 Global Information Security Study documents, economic considerations are actually one of the most important considerations in determining corporate information security spending decisions, and these considerations rate higher than regulatory compliance, company reputation or internal policy compliance, and nearly as high as the number one issue, business continuity/disaster recovery.

Despite the obvious importance of understanding cyber security economics in the development of public policy, it is little discussed and often difficult to delineate.

For example, in order to attack their ultimate targets, it is common practice for cyber attackers to capture and use third-party computers. As a result, many attacked computers do not suffer the direct economic consequences of an attack since they are simply being used to facilitate a further attack. Moreover, the defense, of the ultimate targets of an attack is compromised through the interactions with these third-party systems. The owners of the third party computer systems utilized in a cyber attack may not have the economic incentives to adequately invest in their computers' defense since they do not suffer the direct economic costs of a cyber attack.

On the other hand, the defensive investments required of the ultimate targets of cyber attacks can be substantially undermined by the weakness of others with whom they are interconnected, thus reducing the return on investment (ROI) generated by their cyber security spending.

Ultimately, the economics of cyber security are not readily transparent and are poorly appreciated.

There are also substantial internal reasons for failing to recognize the true costs of cyber events. This is true for consumers, businesses and even the federal government.

For example, many consumers have a false sense of security due to their belief that most of the financial impact resulting from the loss of their personal data will be fully covered by corporate entities (such as the banks). In fact, much of these losses is transferred back to consumers in the form of higher interest rates and consumer fees.

Meanwhile, most of our corporate structures are built on outdated models wherein the owners of data do not understand themselves to be

responsible for the defense of that data. The marketing department has data, the finance department has data, the human resources department has data, but, in most instances, these departments think that the security of their data is not their responsibility, but the responsibility of the "IT guys" at the end of the hall. As a result, the financial risk management of cyber events across enterprise settings is not often properly analyzed, nor properly appreciated, and cyber defense is not adequately budgeted.

At the federal government level, there seems to be no appreciation of the enormous financial risk that the government itself shoulders from the prospect of a "cyber hurricane." In reality, the federal government is the de-facto "insurer of last resort," and would be faced with footing virtually the entire financial burden of a massive cyber event.

This lack of financial risk management on the part of the government is similar in kind to the blind eye that many corporate entities turn toward cyber events. In both cases, a conceptually prudent strategy would be to engage in risk transfer techniques (such as the use of insurance), but there is little evidence that this is occurring on a national level.

The interaction of these factors may be at the root of the fact that, despite the increasingly publicized dangers of cyber incursions, nearly half (47%) of all of the enterprises studied in the 2009 Global Information Security Study reported that they are actually **reducing their budgets for information security initiatives**.

These information security spending decreases are taking place even though many enterprises (42%) acknowledge that the "threats to their information security have increased" and more than half of these enterprises (52%) acknowledge that these cost reductions make adequate security more difficult to achieve.

Ultimately, the dispiriting realization, with respect to cyber security economics, is that all of the current economic incentives favor cyber attackers:

Cyber attacks are comparatively cheap and easy to execute.

The profits that can be generated from cyber attacks are enormous.

The cyber defensive perimeter is nearly limitless.

Losses are difficult to assess.

Defense is costly, and, often, does not generate perceived adequate return on investment.

The ISA Cyber Security Social Contract argues that, much like the utility service model, what will be required to address this issue is for the public sector to deploy market incentives to motivate private investment for the purposes of protecting the public interest. The government is charged with the responsibility to provide for the common defense. However, in the cyber world, the government cannot do this alone. They will require private sector cooperation and investment. While some of the investment will come from corporations serving their own private security needs, the extent of investment to serve the broader public needs, due to some of the unique aspects of cyber economics described previously will be greater than what is justified by private sector business plans.

This brings us to the third central truth that, namely:

III. We will need to develop new understandings about government and industry's roles and responsibilities and limitations if we are to address this serious 21st century problem on a sustainable basis.

The government must face some inconvenient truths.

First, the diversified nature of the internet places much of the critical national security operations in private industry's hands. This does not that mean government has a lesser role; it means that government has a different, and, frankly, an even more challenging role.

Second, although US national security is clearly at stake, unilateral US action cannot solve the problem. The Internet is an inherently global technology. In fact, virtually every component of the system is designed, developed, manufactured, or assembled off US shores and is beyond the reach of US government oversight. We must develop a way to construct a secure system out of potentially insecure parts.

Simultaneously, there is an urgent need to move beyond the informal, DC-centered partnerships of the past. While these inside-the-beltway structures have an important place in the system, government must frankly

address industry at a business plan-level. Government needs to provide incentives for industry to invest in security items that may not be justified by their corporate business plans.

The good news is that we know a great deal about how to protect the Internet, and we can achieve tremendous progress rather quickly if we embrace new government and industry roles that are geared toward implementing voluntary compliance with practices, technologies and standards that have been independently-proven to be effective.

There is a wide range of evidence that the market has already generated the practices/standards and technologies that can address most of the cyber security problem. What we have yet to address are the economics of the problem.

The "Global Information Security Survey" conducted by PricewaterhouseCoopers found that organizations that followed best practices had zero downtime and zero financial impact, despite being targeted more often by malicious actors.

An almost identical finding was reported in the "2008 Data Breach Investigations Report" conducted by Verizon. This study drew on over 500 forensic engagements over a four year period, including literally tens of thousands of data points. The study concluded that, in 87% of cases, investigators were able to conclude that the breach could have been avoided if reasonable security controls had been in place at the time of the incident."

Robert Bigman, the CIA's Chief of Information Assurance, told attendees at an Aerospace Industries Alliance meeting this October that, contrary to popular belief, most attacks were not all that sophisticated. He estimated that with the use of "due diligence" you could reject between 80 and 90% of attacks. "The real problem is implementation," said Bigman.

So what is the best role for government to play in this new digital world?

To begin, Congress ought to heed President Obama's admonition, and not mandate cyber security standards for the private sector.

Apparently, there is still a belief among some of the digital immigrants around Capitol Hill that there must be some single, minimum, gold standard of cyber security that the government ought to mandate. There is not.

This is not to say that there are not standards that work. In fact, the joke in the cyber security world about standards is, the good thing about cyber security standards is that there are so many of them.

And, there is a reason for the multitude of standards and practices. Modern systems are not fully purchased off the shelf and then plugged into the wall like a TV. Enterprises are constantly modifying their systems internally, upgrading some portions of the systems and not others, and adapting these systems to fit various business models, competitive climates, and various contractual, cultural, and regulatory regimes. There is no one size fits all.

In truth, though, the government really ought not to care about what the standards are, or, even, who created them. What government ought to care about is what works.

The broad model we suggest that the government consider is that of the FDA, which does not create drugs, and instead evaluates drugs for efficacy. This is a role for the federal government to fulfill, although not directly. The federal government ought to fund the independent evaluation of cyber security standards, practices, and technologies so the private sector will know both what works and how well. Then, it should be completely up to private enterprises to select what they choose to adopt voluntarily.

The second role the government ought to undertake is to modernize the economic incentive structures so that they are geared to protecting both our immediate and long-term national economic and defense issues.

Again, in this regard, we support the initial steps that have been outlined in the Administration's Cyber Space Policy Review. ISA has developed a fairly detailed outline of how this system ought to work, which I have abstracted for our written testimony.

A third area for governmental involvement is with respect to education. Again, this is well-emphasized in the Administration's

document. However, I would make this area a point of caution. There is currently, by senior policy makers, a lot of talk about the need for cyber education among k-12 students. As the father of young children, I, myself, naturally support these efforts, especially if they focus on values and principles.

The caution is that these digital natives, who are in the k-12 quadrant, tend to be on average much more technology savvy than many of the digital immigrants who are their teachers.

We would suggest that the government pay greater attention to enterprise education as that will reach the people who are in the work force now, many of whom will be there for decades. This population is also among the main digital immigrants - especially the senior executives. Far more immediate and long-term return on investment might be gained through a sophisticated Enterprise Education program, along the lines mentioned in the Cyber Space Policy Review, than through in-depth k-12 cyber security education.

Finally, I would like to turn to how to create a functioning government industry partnership that is based on market incentives and will reach industry where the key decisions are made - at the business plan level.

In order to create a system to maximize the use of market incentives for cyber security, three essential elements need to be developed.

1. A system must be developed to determine, on an ongoing basis, what voluntary behaviors will merit incentives.
2. A network of incentives must be catalogued and then applied to the widely diverse private sector.
3. A system to monitor use of the voluntary regime must be developed in order to track the appropriateness and the effectiveness of the incentives.

ISA proposes a system that will address each of these areas:

1. Determining what actions deserve incentives

The best way for government to motivate the specific cyber security behaviors it would like industry to adopt to meet the national (i.e. beyond

61662.071

normal business) interests, is to engage industry at the business plan level and to make it in the private corporation's best economic interests to enhance the infrastructure.

An effective method of stimulating security would be to create a competitive market for the development, and the adoption of sound security practices, standards, and technologies.

By creating a competitive market, the power of that market can be harnessed to motivate improved cyber security and, since many of the organizations targeted are international, improvements on a worldwide basis are quite possible.

The government, as well as the private sector, would create market incentives for higher tiers of standards and practices to be utilized within businesses by designating contractual requirements that matched the criticality of a product/program to a given security posture (e.g., a contract for critical infrastructure might require a Tier 4 certification while a contract for paper products might only require Tier 1).

Such a model would provide incentives for individual companies to invest, on purely voluntary basis, in enhanced cyber security in order to access even higher levels of incentives.

ISA proposes that government identify multiple entities, both public and private, to identify standards and practices that would be eligible for market incentives.

Also, it is important that the government not declare a single set of standards. Government can be subject to political pressure, and it can be a challenge for government to deal with the vast and ever-changing array of needs that face companies, many of which are not US-based but actively contribute to the US economy. In addition, there may likely be strong international resistance to standards that are solely determined by the US government. Perhaps more important, though, the notion of one-size fits all does not recognize the reality of multiple business sizes, cultures, regulatory regimes, and degrees of criticality within the infrastructure and business plans.

The government's first role would be to select and fund independent research of the interventions created by the approved agencies. Entities would be able to remain on the list of qualifying standards and practices only based on the efficacy of their standards as determined by independent studies.

At the outset, we propose that federal incentives be available to companies if they implement information security pursuant to, and meet the:

- Information security procedures adopted for regulated services by a Federal sector-specific regulatory agency.

- Standards established and maintained by the following recognized standards organizations such as:
  - International Standards Organization
  - American National Standards Institute
  - The Internet Security Alliance
  - National Institute of Standards and Technology

- Standards established and maintained by an accredited security certification organization, or a self-regulatory organization such as NASD, BITS, or the PCI structure.

- Technologies approved as designated or certified anti-terror technologies by the Department of Homeland Security under the SAFETY Act.

- Private entities, such as insurance and audit firms, who can demonstrate either a financial interest in quality compliance or independent research.

Various incentives would be awarded to enterprises based on the quality of the practices they have voluntarily chosen to implement.

The ISA model is superior for many reasons:

First, it allows for multiple "standards" to be rewarded and, thus, avoids the one size fits all problem of a single standard.

Second, standard-setting organizations would compete to continually improve their standards and their cost effectiveness in order to receive better grades and to qualify their users for improved incentives. The standard setting entities themselves are enhanced by the number of organizations that adopt their standards.

As a result, there is a continuing economic motivation to improve the "standards/practices/technologies." This has a social benefit since technologies, along with their vulnerabilities and threat vectors, also constantly change. While traditional regulatory mechanisms move far too slowly to keep pace with this continuing evolution, a system motivated by profit can move with far greater speed.

Third, international standards can qualify for US incentives, which will better meet the needs of international corporations and will side-step the problems of a US-only implementation or the setting of bad precedent.

Fourth, while the US cannot "govern" foreign operating organizations, it can provide incentives for good behavior to them or to US domestic entities in their non-domestic facilities. As a result, an incentive system will allow the US to improve not only domestic cyber security, but also international cyber security, which is in the US' national interest.

2. Creating a system of incentives that can be matched to various, individualized corporate needs and levels of voluntary security compliance.

It is important to note at the outset, that the use of market incentives to promote cyber security does not necessarily mean large government spending increases. For example, in many instances, such as SBA loans or special instances such as the awarding of TARP money, the government is making the expenditure already and would simply be adding to the requirements for recipients. In addition, there are a variety of non-monetary incentives, including streamlined regulation and liability protections, that don't entail any direct costs. Finally, there is a range of private sector incentives, such as insurance, that can be far better developed and can be used to improve cyber security just as other such mechanisms have been used to enhance health, driving, and other consumer behavior.

In the ISA model, various tiers of standard/practice compliance could then be mapped to the qualifying incentives for these various levels of compliance (e.g., level "x" yielding tax incentive "a," and level "y" yielding tax incentive "b").

However, just as it is true that one size of standard/practice may not apply equally well to various businesses or technology systems, it is also true that one set of incentives may have different applicability and attractiveness to different enterprises.

Obviously, a defense contractor might be most attracted by incentives tied to government procurement, whereas a financial institution might be more attracted to insurance benefits and smaller companies might be more interested in expanding the opportunity to access SBA loans. The list of examples can go on and on.

As a result, ISA suggests that a range of incentives ought to be made available to those companies that choose to enhance their own security.

The following is a list of incentives, many of which are of low or virtually no-cost to the public that can be used to alter economic perspective with respect to investment in cyber security procedures, and, thus, encourage private entities to improve their security posture in the broad national interest.

1. Create a Cyber Safety Act. The SAFETY Act, passed after 9/11 to spur the development of mostly physical security technology by providing marketing and insurance benefits, could be adapted to provide similar benefits for the design, development, and implementation of cyber security technology, standards, and practices.

By designating or certifying organizations under the SAFETY Act for developing or using cyber security technology, practices, and standards, these organizations can similarly use the marketing and insurance benefits, thereby providing business benefits to extending their cyber security spending beyond what is initially justified by their business plans. The program has been successful in the physical arena.

2. Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices.

Using the model described previously for selecting standards and practices, make on-going eligibility for federal grants and loans contingent on compliance with identified security practices. This is a proven, and successful method for advancing broad policy objectives (e.g., non-discrimination in employment).

One of the benefits of this approach is that there is no significant impact on the federal budget due to the fact that this money is already designated for distribution. There is also the potential for relatively immediate impact since this approach utilizes current standards, practices, and government programs. In addition, this approach allows for adaptation to future needs since most applications must be periodically renewed. Finally, a renewal process in place for these types of government contracts will allow for compliance testing as a means of approving and of continuing the contracts. The reach of the positive effect of this approach will go beyond major players to include a broader universe of suppliers and contractors to CIKR.

3. Leverage Purchasing Power of Federal Government. Government could increase the value of security in the contracts it awards to the private sector, thereby encouraging broader inclusion of security in what is provided to government. This approach could facilitate broad improvement of the cyber security posture among CIKR owners and operators by "building in" security at inception in products and services that are developed and delivered to the government. If the requirements were extended to suppliers and sub-contractors as well, this initiative could also have a significant effect on down-stream entities.

While this approach does have the potential for substantial benefits, government needs to enhance the value of the contracts because a number of the organizations within the supply chain do not have the same massive incentive to adopt government specifications that some larger players do. This approach has potential for real and immediate benefits, but it is important that government realize that such compliance cannot be expected to come "for free." National security has a cost, and that cost is the government's responsibility.

4. Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks that address information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance

Portability and Accountability Act, along with state regimes, could be analyzed to create a unified compliance mode for similar items and to eliminate any overlaps. Sector-specific requirements could be identified, of course, but effective security has many similar elements. Duplicative regulations would impose a cost on industry that, ultimately, increases its resistance to prioritizing compliance.

If compliance with one set of regulations were to be considered compliance with all, the reduction in compliance costs would allow for the freeing-up of resources to be returned to security efforts as opposed to compliance efforts.

5. Tax incentives for the development of, and compliance with cyber security standards practices and use of technology. Using our model for selecting standards and practices as described previously the receipt, and on-going eligibility for tax credits can be made contingent upon compliance with identified security practices.

While tax incentives are often difficult politically, this approach may be targeted to small and medium-sized businesses. SMEs are a weak link in the cyber security supply chain and, without incentives, they may never perceive compliance with effective cyber security practices to be economically beneficial.

6. Grants/Direct Funding of Cyber Security R&D. The Federal Government could give grants to companies that are developing and implementing cyber security technologies or practices. Alternatively, R&D could be run through one or more of the FFRDCs. This approach would reduce the private-sector cost of developing and deploying cyber security technologies.

7. Limit liability for good actors. The Federal Government could create limited liability protections for certified products and processes, such as those approved under the modified SAFETY Act proposal, or those certified against recognized industry best practices. Alternatively, liability might be assigned on a sliding scale (comparative liability), such as limiting punitive damages while allowing actual damages, and providing affirmative defenses with reduced standards (preponderance of evidence vs. clear and convincing etc.).

Liability costs are among the most sensitive issues confronting senior corporate executives, and these costs are a long-standing target for reform. Tying adherence to best practices and standards to a limitation in liability might be extremely effective in building a business case for extended cyber security investment. There is no such thing as perfect security, but one of the biggest concerns within industry is that, despite making the best possible investments in security, a court would still impose liability for a successful, one-in-a-million hostile attack. This type of outcome is not in the best interest of the public policy for improving security.

In making this proposal, our objective is to provide incentives to those who make authentic investments in improved security consistent with the standards and best practices that are incorporated into an overall government program. This objective stands in contrast to those who argue that there should be no liability at all.

8. Create A National Award for Excellence in Cyber Security. The Federal Government could create an award for companies that adopt cyber security best practices (e.g., the Malcolm Baldridge Award by the Department of Commerce).

This is a low-cost effort with substantial benefits. Organizations may strive to receive the award as a means of differentiating themselves in marketing, and consumers will most likely value companies that have this type of recognition, particularly in a marketplace in which security concerns continue to increase.

9. Promote Cyber Insurance. Cyber insurance, if more broadly utilized, could provide a set of uniform and constantly improving standards for corporations to adopt and to be measured against, all while simultaneously transferring a portion of risk that the Federal Government might face in the case of a major cyber event. Insurers require some level of security as a precondition of coverage, and companies that are adopting better security practices will receive lower insurance rates. This helps companies to internalize both the benefits of good security as well as the costs of poor security, which in turn leads to greater investment and improvements in cyber security. The security requirements utilized by cyber-insurers are also helpful in this regard.

With widespread take-up of insurance, these requirements will become de facto standards, while still being responsive to updates that are necessary in the face of new risks. Insurers have a strong interest in greater security, and their requirements are continually increasing. In addition to directly improving security, cyber-insurance is also enormously beneficial in the event of a large-scale security incident.

Insurance provides a smooth funding mechanism for recovery from major losses, helping businesses return to normal and to reduce their need for government assistance. Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater and lower premiums for companies whose expected loss is lower. This avoids a potentially dangerous concentration of risk, while also preventing companies from gaining a free-ride. Insurance companies can also provide a market-based monitoring and assessment function that reduces the cost to the government while assuring compliance with ever-increasing standards and practices.

3. A system to monitor use of the voluntary regime must be developed in order to track the appropriateness and the effectiveness of the incentives.

It is sometimes blithely asserted that if the private sector doesn't do a better job of monitoring cyber security, the government will simply have to regulate it.

Often these assertions are followed by suggestions that Sarbanes/Oxley, GLB, or HIPAA standards could simply be expanded.

Leaving aside the broad policy problems with these simple solutions research suggests that such expansion of government regulation is unlikely to succeed if enacted.

The PricewaterhouseCoopers study, as reported in the October 2008 edition of CIO Magazine, claims that only "44% of respondents say they test their organizations for compliance with whatever laws and industry regulations apply." The study notes that this represents an increase in compliance, but it is extremely noteworthy that, several years after these laws and their regulations (such as HIPAA and Sarbanes-Oxley) have been in effect, less than half of the surveyed companies are even testing for compliance.

CIO magazine goes on to note, "many organizations aren't doing much beyond checking off the items spelled out in regulations - and basic safeguards are being ignored," which is consistent with the findings of the 2008 Data Breach Investigations Report cited earlier.

The federal government's lack of success in getting federal agencies to meet their own FISMA requirements also suggests that this is not an area in which the federal government performs well. As such, it is impractical for the federal government, funded only by tax dollars, to take on the massive role of determining, monitoring, and constantly adjusting cyber security requirements.

A far more practical approach would be for the federal government to use its resources to establish a functional private sector system in which the federal government could participate, and, where necessary, regulate. Insurance companies are the best available vehicle for such a program.

The insurance industry is uniquely motivated to understand and communicate to its insured what standards of due care are appropriate for the management of network security because the industry has "skin in the game." That is to say, in the event of a loss, it is the insurance company that will pay the excess of any self-insured retention and any damages to third parties, as well as reimburse the policyholder for any loss of business and any additional expenses associated with the event.

A robust cyber insurance industry, operating under traditional regulatory regimes, could serve the public interest by providing a mechanism for the continual upgrading of security practices and standards, the monitoring of compliance, and the reduction of government's risk exposure in the event of a cyber hurricane.

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
On The Subcommittee On Terrorism And Homeland Security's Hearing On
"*Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace*,"
November 17, 2009

I commend Senator Cardin and the Subcommittee on Terrorism and Homeland Security for holding this timely hearing on "*Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace.*" The troubling cyber attack on U.S. Government computers in July was an important reminder that developing a comprehensive national strategy for cybersecurity is one of the most challenging and important issues facing our Nation. Just last week, the Government Accountability Office released a report finding that the computer network at the Los Alamos National Laboratory remains vulnerable to cyber attack.

The Judiciary Committee has made improving the security of our Nation's computers one of its highest legislative priorities. Earlier this month, the Committee reported comprehensive data privacy legislation that will help to better secure the Nation's computer systems and to protect privacy. Today's hearing on cybersecurity builds upon the Committee's work in this area.

I am particularly pleased that this hearing will examine the need to balance the effort to improve cybersecurity with our obligation to protect the privacy rights and civil liberties of all Americans. I have long believed that national security and personal liberty are not mutually exclusive. We can -- and must -- have both in a vibrant Democracy.

A key tool put in place by the Congress to ensure both security and liberty is the Privacy and Civil Liberties Oversight Board – a critical board established by the Congress to ensure that privacy and civil liberties concerns are appropriately considered in developing and implementing the Nation's counterterrorism policies. In May, the President's report on Cyberspace Policy Review recommended that this Board be quickly reconstituted and that its work include cybersecurity-related issues.

Having a fully functional Privacy and Civil Liberties Oversight Board is vital to protecting the privacy and civil liberties of all Americans and to developing a comprehensive national cybersecurity strategy. That is why I have urged the President to promptly appoint qualified individuals to this Board.

The testimony offered today will help the Committee as it continues its oversight of emerging cybersecurity issues involving the Departments of Justice and Homeland Security and the President's new cybersecurity initiative. I thank all of the witnesses for sharing their insights on this emerging issue with the Committee.

I also thank Senator Cardin for his leadership on the issue of cybersecurity. I look forward to a meaningful exchange.

#####

Statement of Gregory T. Nojeim

Senior Counsel and Director,
Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the Senate Committee on the Judiciary,
Subcommittee on Terrorism and Homeland Security

on
Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace

November 17, 2009

Chairman Cardin, Ranking Member Kyl and Members of the Subcommittee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology.[1] We applaud the Subcommittee's leadership and foresight in examining the challenges we face as a nation in preventing terrorist attacks in cyberspace in a manner that also protects privacy and civil liberties. Today, I will briefly outline the cybersecurity threat and explain why measures appropriate for securing some critical infrastructure systems would be inappropriate for others. I will emphasize that private network operators, not the government, should monitor and secure private sector systems, while the government should monitor and secure its networks. I will discuss some incremental changes in the law that may enhance information sharing without eroding privacy. Finally, I will discuss the role that identity and authentication measures, if properly designed and deployed, can play in enhancing security while also protecting privacy.

The Cybersecurity Threat

It is clear that the United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. Just last week, the news magazine *60 Minutes* brought the cybersecurity threat into Americans' living rooms, reporting that cyber thieves had stolen millions of dollars from banks and key secrets from the government.[2] Earlier this year, the *Wall Street*

---

[1] The Center for Democracy & Technology is a non-profit, public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom after September 11, 2001. CDT coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications and public interest organizations, companies and trade associations interested in information privacy and security issues.

[2] http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00119 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.082

Journal reported that computer hackers had penetrated systems containing designs for a new Air Force fighter jet and had stolen massive amounts of information.[3] U.S. intelligence agencies, which have developed capabilities to launch cyber attacks on adversaries' information systems, have sounded alarms about what a determined adversary could do to critical information systems in the U.S.

It is also clear that the government's response to this threat has been woefully inadequate. While we welcome the leadership of Secretary Napolitano and Deputy Undersecretary Reitinger, the Department of Homeland Security has been repeatedly criticized[4] for failing to develop plans for securing key resources and critical infrastructure, as required in the Homeland Security Act of 2002.[5] President Obama's national security and homeland security advisors completed a cyberspace policy blueprint on April 17, making many useful recommendations, but implementation of those measures has been slowed by the Administration's failure to appoint the cybersecurity official in the White House who could drive policy development and coordinate implementation of a government-wide plan.

The Subcommittee can play an important role in addressing some of the gaps in cybersecurity policy.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. It is absolutely essential to draw appropriate distinctions between government systems and systems owned and operated by the private sector. Policy towards government systems can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

---

[3] Gorman, Siobhan, Computer Spies Breach Fighter-Jet Project, *The Wall Street Journal*, http://online.wsj.com/article/SB124027491029837401.html, April 21, 2009. *See also,* Gorman, Siobhan, Electricity Grid in U.S. Penetrated by Spies, *The Wall Street Journal*, http://online.wsj.com/article/SB123914805204099085.html, April 8, 2009.

[4] *See, e.g.,* Government Accountability Office, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* http://www.gao.gov/new.items/d061087t.pdf, Testimony of GAO's David A. Powner, Director, Information Technology Management Issues, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, September 13, 2006. Last year, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team, which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, http://www.gao.gov/products/GAO-08-588, July 2008.

[5] P.L. 107-296, Section 201(d)(5).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00120 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.083

With respect to private systems, it is further necessary when developing policy responses to draw appropriate distinctions between the elements of "critical infrastructure" that primarily support free speech and those that do not. The characteristics that have made the Internet such a success – its open, decentralized and user controlled nature and its support for innovation, commerce, and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all "critical infrastructure."

While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the network into the same basket. For example, while it is appropriate to require authentication of a user of an information system that controls the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers.

In sum, CDT believes that cybersecurity legislation and policy should not treat all critical infrastructure information systems the same. Instead, a sectoral approach is called for. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet and communications structures critical to new economic models, human development, free speech and privacy are not regulated in ways that could stifle innovation, chill free speech or violate privacy.

Network Providers – Not the Government – Should Monitor Privately-Owned Networks for Intrusions

When the White House released the Cyberspace Policy Review on May 29, President Obama said:

> *"Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."*

CDT strongly agrees. No governmental entity should be involved in monitoring private communications networks as part of a cybersecurity initiative. This is the job of the private sector communications service providers themselves, not of the government. Most critical infrastructure computer networks are maintained by the private sector. Private sector operators already monitor those systems on a routine basis to detect and respond to attacks and as necessary to protect their networks, and it is in their business interest to continue to ramp up these defenses. Indeed, providing reliable networks is essential to maintaining their business.

Current law gives these service providers substantial authority to monitor their own systems and to disclose to the government and to their peers information about

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00121 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.084

cyberattack incidents for the purpose of protecting their own networks. Appropriately, the law does not authorize ongoing, routine disclosure of traffic. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider. 18 U.S.C. 2511(2)(a)(i). This includes the authority to disclose communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications (18 U.S.C. 2702(b)(3)) and customer records (18 U.S.C. 2702(c)(5)) to any governmental or private entity.[6] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[7] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass. 18 U.S.C. §2511(2)(i). The subcommittee should explore with service providers how they interpret and apply these provisions in the cybersecurity context.

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to the government. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. Should the Subcommittee find that there is any confusion or ambiguity about this, it should consider amending these provisions to make it clear that they permit, in regards to cybersecurity, disclosure only of information relating to a suspected attack or other particular cybersecurity threat. The Subcommittee should also consider requiring public, statistical reporting on the use of these provisions to assure the public that these authorities do not devolve into a backdoor governmental monitoring system.

There is a widespread perception that cybersecurity information sharing as practiced is inadequate and there is some concern that the provisions of the Wiretap Act and ECPA are impediments to information sharing. We urge the Subcommittee to approach this issue very cautiously, for exceptions intended to promote information sharing could end up severely harming privacy. First, it should be noted that there has not been sufficient analysis to determine what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing

---

[6] Another set of exceptions authorizes disclosure if "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications [or information] relating to the emergency." 18 U.S.C. 2702(b)(8) and (c)(4).

[7] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. 2510(21).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00122 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.085

structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[8] and the public-private partnerships represented by the Information Sharing and Analysis Centers (ISACs)[9] are inadequate. The Government Accountability Office (GAO) recently made a series of suggestions for improving the performance of U.S. CERT.[10] The suggestions included giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Secondly, it seems that industry self-interest, rather than government mandate, should be relied on to facilitate information sharing. The Subcommittee should explore whether additional market-based incentives could be adopted to encourage the private sector to share threat and incident information and solutions. Since such information could be shared with competitors and may be costly to produce, altruism should not be expected, and compensation may be appropriate. One option, therefore, would be to compensate companies that share with a clearinghouse the cybersecurity solutions in which they have invested substantial resources. The Subcommittee might also consider whether an antitrust exemption to facilitate cybersecurity collaboration is necessary. Other options would be to provide safe harbors, insurance benefits and/or liability caps to network operators that share information about threats and attacks in cyberspace by terrorists and others.

---

[8] U.S. CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments.

[9] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established Information Sharing and Analysis Centers (ISACs) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. *See*, THE ROLE OF INFORMATION SHARING AND ANALYSIS CENTERS (ISACS) IN PRIVATE/PUBLIC SECTOR CRITICAL INFRASTRUCTURE PROTECTION 1 (Jan. 2009), *available at* http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

[10] *See* Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, http://www.gao.gov/products/GAO-08-588, July 2008.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00123 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.086

CDT strongly disagrees with proposals to solve the information sharing dilemma by simply expanding government power to seize privately held data. We urge the Subcommittee to steer clear of a recent proposal to give the Secretary of Commerce unfettered authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities, regardless of whether the information to be accessed is proprietary, privileged or personal and without regard for any law, regulation or policy that governs governmental access, including privacy laws like the Electronic Communications Privacy Act.[11] Such an approach would be dangerous to civil liberties and would undermine the public-private partnership that needs to develop around cybersecurity. Collecting large quantities of sensitive information into a common database can also undermine security because such a database could, itself, become a target for hackers.

While, as noted above, current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, we have heard concern that the provisions do not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. Many types of attacks could affect multiple providers, and disclosure by one entity about such an attack could be helpful to others. Therefore, there might be a need for a very narrow exception to the Wiretap Act and ECPA that would permit such disclosures about specific attacks and malicious code on a voluntary basis, and that would immunize companies against liability for these disclosures. The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited.

Overall, given the risks to privacy, we urge the Subcommittee to take only incremental approaches to information sharing, avoiding more radical approaches, such as permitting or mandating broad sharing of information that may be personally identifiable. In addition, because the existing privacy protections in ECPA have been outpaced by the development of technology, we urge the Subcommittee to ensure that any changes to the statute to facilitate cybersecurity measures are counterbalanced with enhanced privacy protections.

The government also has a legitimate role, to the extent it has any special expertise, in helping the private sector develop effective monitoring systems to be operated by the private sector. The government should be sharing information with private sector network operators that will help them identify attacks at an early stage, defend in real time against attacks, and secure their networks against future attack. Most of the federal government's cybersecurity effort regarding private sector networks should focus on improving information sharing and otherwise strengthening the ability of the private sector to protect private sector networks.

---

[11] Section 14 of the Cybersecurity Act of 2009, S. 773.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00124 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.087

Some have proposed that the President ought to be given authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of national security.[12] Such extraordinary power should extend only to governmental systems (presumably, the government already has the authority to disconnect its own systems from the Internet), but should not extend to those maintained by private sector entities. Even if such power over private networks was exercised only rarely, its mere existence would pose other risks, enabling a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system. Any such shut down could have far-reaching, unintended consequences for the economy, for the critical infrastructures themselves, and for users of those systems, which may include government personnel, state and local emergency personnel, first responders, and civilian volunteers. It could even discourage private sector operators from quickly shutting down their own networks when they should out of fear of liability for doing so, as they wait to see whether the President will order the shut down. To our knowledge, no circumstance has yet arisen that could justify a Presidential order to limit or cut off Internet traffic to a particular critical infrastructure system when the operators of that system think it should not be limited or cut off. They already have control over their systems and financial incentives to quarantine network elements that need such measures. We urge you to reject proposals to give the President or another governmental entity power to limit or shut down Internet traffic to privately-held critical infrastructure systems.

The Government Should Monitor Its Own Networks for Intrusions, But Privacy Concerns Need to Be Addressed

Just as private sector network operators should, and do, monitor their systems for intrusions, the federal government clearly has responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that if communications Americans have with the government are routinely accessed and often shared with law enforcement and intelligence agencies, this will chill the exercise of the First Amendment rights of free speech and to petition the government. Some methods of detecting intrusions raise more privacy concerns than do others. While the Fourth Amendment may not come into play because those communicating with governmental entities necessarily reveal their communications – including content – to the government, the privacy and civil liberties inquiry does not stop there. Protecting privacy in this context is absolutely critical to giving Americans the necessary comfort to communicate with their government.

Another important consideration is the question of how likely it is that private-to-private information may be accessed inadvertently through systems intended to detect intrusions against government computers. The role of intelligence and law enforcement agencies such as the NSA and the FBI in the intrusion detection

[12] Section 18 of the Cybersecurity Act of 2009, S. 773.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00125 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.088

enterprise must be carefully considered. Generally, the principles of Fair Information Practices should be applied to minimize the amount of personally-identifiable information collected by the government, to limit its use of this information, and to notify users of the information collection and disposition.[13]

Under current law, all federal departments and agencies must adhere to information security best practices. Generally these practices include the use of intrusion detection systems.[14] In an effort to improve security, the government has developed and is deploying a new intrusion detection system called "Einstein 2." According to a May 19, 2008 Privacy Impact Assessment,[15] and to a January 9, 2009 opinion of the DOJ Office of Legal Counsel,[16] Einstein 2 will be deployed at participating federal agency Internet Access Points.[17] Its first full implementation was at the Department of Homeland Security. Five other federal agencies were supposed to begin using it by June 2009.[18] Einstein assesses network traffic against a pre-defined database of signatures of malicious code and alerts U.S. CERT to malicious computer code in network traffic. While the signatures are not supposed to include personally identifiable information ("PII") as defined by DHS, they do include IP addresses, and the alerts that Einstein 2 generates for U.S. CERT may include PII.[19] In addition to

---

[13] Department of Homeland Security's Chief Privacy Officer issued a memorandum in late 2008 to describe how DHS would apply FIPS. *Privacy Policy Guidance Memorandum,* issued December 29, 2008 by Hugo Teufel III, Chief Privacy Officer, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[14] Einstein 2 PIA, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf (May 19, 2008), p. 2.

[15] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf.

[16] Stephen. G. Bradbury, Principal Deputy Assistant Attorney General, *Legal Issues Relating To the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch,* January 9, 2009, http://www.justice.gov/olc/2009/e2-issues.pdf. The memo concludes that operation of Einstein 2 does not violate the Constitution or surveillance statutes, and an August 14, 2009 opinion from the Obama Justice Department's Office of Legal Counsel affirms that conclusion. http://www.justice.gov/olc/2009/legality-of-e2.pdf.

[17] It is unclear whether this means that Einstein 2 operates on privately owned and operated equipment or on government equipment. More importantly, it is unclear whether the network points at which Einstein is deployed handle only government traffic or could carry both government and private-to-private traffic.

[18] http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/16jun/Fonash_Testimony.pdf, p. 5.

[19] The PIA for Einstein 2 makes it clear that, for example, Einstein 2 will collect an email address when the source of malicious code it detects is attached to an email address. Moreover any "flow record" (a specialized summary of a suspicious communication) that

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00126 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.089

using attack signatures, Einstein 2 also detects anomalies from the norm in network traffic on a particular system and alerts U.S. CERT to those anomalies.

Press reports in the *Washington Post*[20] and *Wall Street Journal*[21] indicate that the federal government is developing a successor intrusion detection system, dubbed "Einstein 3." This new system will also rely on pre-defined signatures of malicious code that may contain PII. However, while Einstein 2 merely detected and reported malicious code, Einstein 3 is to have the capability of intercepting threatening Internet traffic before it reaches a government system, raising additional concerns.

Given these capabilities, a key question is where Einstein operates – on network elements that carry only government traffic or on elements where it might scan private-to-private communications – and how likely it is to scan private-to-private communications. According to press accounts, Einstein 3 will operate inside the networks of the telecoms. Thus, one critically important question is whether Einstein can reliably focus on communications with the government to the exclusion of private-to-private communications. If Einstein were to analyze private-to-private communications, that would likely be an interception under the electronic surveillance laws, requiring a court order. The Subcommittee may want to consider legislation that would require that an independent audit mechanism be put in place as part of Einstein 3 or any similar system to ensure that no private-to-private communications are scrutinized, and require a report to Congress if they are.

Other questions about the Einstein intrusion detection system include:

- What personally-identifiable information that Einstein 2 has collected so far?
- What have law enforcement and intelligence agencies done with Einstein information that is shared with them, and more to the point, to what extent is the system being used to identify people who should be prosecuted or people who are of intelligence interest, even if that is not its primary purpose?
- To what extent are private sector operators keeping information about communications that appear to match attack signatures?
- How should users be notified that their visits to government websites and their email communications with government employees are being scanned for security reasons? [22]

Einstein routinely generates will generally include IP address and time stamp, which are widely regarded as personally identifiable.

[20] http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771_pf.html.

[21] http://online.wsj.com/article/SB124657680388089139.html#printMode.

[22] For a fuller listing of open questions about the Einstein Intrusion Detection System, see Center for Democracy & Technology, *Einstein Intrusion Detection System: Questions That Should Be Addressed*, http://www.cdt.org/security/20090728_einstein_rpt.pdf.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00127 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.090

The Senate version of the Intelligence Authorization Act for FY 2010 seeks answers to similar questions. It calls for reports to Congress about the privacy impact of Einstein and any other similar cybersecurity programs as well as information about the legal authorities for the programs and about any audits that have been conducted or are planned for the programs.[23] At any rate, the Department of Homeland Security should, of its own initiative, publish an unclassified Privacy Impact Assessment of Einstein 3, as it did for Einstein 2.

The lack of transparency around Einstein highlights a broader concern about the federal government's cybersecurity program: excessive secrecy undermines public trust and communications carrier participation, both of which are essential to the success of the effort. The government needs to publicly disclose sufficient details about Einstein and other programs to be able to assure both the public at large and private sector communications service providers that the confidentially of personal and proprietary communications will be respected.

Role of the NSA in Securing Unclassified Civilian Systems

Some have suggested that the National Security Agency should lead or play a central role in the government-wide cybersecurity program. They argue that the NSA has more expertise in monitoring communications networks than any other agency of government. However, expertise in spying does not necessarily entail superior expertise in cybersecurity. Moreover, there is serious concern that if the NSA were to take the lead role in cybersecurity for civilian unclassified systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, increasing the likelihood of failure or of ineffectiveness.

NSA is committed, for otherwise legitimate reasons, to a culture of secrecy that is incompatible with the information sharing necessary for the success of a cybersecurity program. For these reasons, among others, NSA should not be given a leading role in monitoring the traffic on unclassified civilian government systems, nor in making decisions about cybersecurity as it affects such systems; and its role in monitoring private sector systems should be even less. Instead, procedures should be developed for ensuring that whatever expertise and technology NSA has in discerning attacks is made available to a civilian agency.[24]

---

[23] S. 1494 as passed by the Senate on September 16, 2009 http://intelligence.senate.gov/090722/s1494.pdf. *See* Section 340. The Senate Select Committee on Intelligence Report on the bill, 111-55, can be found here: http://intelligence.senate.gov/090722/2010report.pdf. *See* p. 22. The House version of the bill does not include a similar provision.

[24] CDT does not quarrel with the role the NSA Chief has been given as commander of the new United States Cyber Command in the Department of Defense. Securing military systems seems a proper role for the NSA.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00128 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.091

The lead for cybersecurity operations should stay with the Department of Homeland Security, and DHS's National Cyber Security Center (NCSC) should be provided with the necessary resources.

Building Privacy Into Identity and Authentication Requirements Designed To Thwart or Discourage Malicious Activity

One of the most talked-about approaches to preventing and tracing cyber attacks by terrorists and others is to improve identity and authentication of those who would seek access to the system that must be protected. If an attack cannot be attributed to a particular person because the person cannot be identified, it is difficult to prosecute the perpetrator. While identification and authentication will likely play a significant role in securing critical infrastructure, identity and authentication requirements should be applied judiciously to specific high value targets and high risk activities.

Some have argued for broad authentication mandates across the Internet – including calls for "Internet passports." Mandating strong identity and authentication measures for routine Internet interactions could seriously compromise user privacy, slow on-line interactions and transactions so much that their utility would be impaired, and fundamentally limit the ways in which people use the Internet.

While identity and authentication measures are important elements of cybersecurity, they can either promote privacy or threaten it, depending on how they are designed and implemented. For example, the fact that a transaction or interaction cannot be traced to an identifiable individual may enhance privacy and security. Moreover, the right to speak anonymously enjoys constitutional protection.[25] On the other hand, authentication can also enhance privacy. For example, authenticating a party to a transaction may advance a privacy interest by preventing identity fraud. Depending on how the authentication system is designed, disclosing personally-identifiable information to facilitate authentication may put privacy at risk or it may increase privacy. For example, it is possible to disclose data to establish trusted credentials that can be used for many on-line transactions, thereby eliminating the need to provide such information for each transaction and to many different entities.[26] Instead of submitting personal information to 10

---

[25] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995).

[26] Center for Strategic and International Security, *Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf, December, 2008, p. 63. The CSIS report advocates strong authentication of identity for the information and communications technology sector, and the energy, finance and government services

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00129 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.092

websites in order to make 10 purchases, the information could be submitted once to a credentialing organization that would perform the authentication necessary to the other transactions. Huge design and implementation issues must be addressed to ensure that such a system enhances privacy and security rather than undermining them.

Identity and authentication requirements should adhere to the principles of proportionality and diversity.[27] Under the proportionality principle, if a transaction has high significance and sensitivity and an authentication failure carries with it significant risk, it may be more appropriate to require authentication and the collection of more sensitive information to authenticate. Conversely, certain transactions do not need high degrees of authentication, if any. This principle applies in both the private and public sectors, but private sector operators – who know their systems best – are in the best position to decide what level of identity and authentication should be required for their own systems and transactions, depending on the degree of risk posed and the degree of trust that is called for. Private sector operators, such as those in the financial sector, already use various security measures related to online services such as banking and e-commerce. In addition, in light of the federal government's poor historical track record on securing its own systems, it may not be the best entity to put in charge of credentialing or other centralized online security activities.

The Office of Management and Budget E-Authentication Guidance for Federal Agencies[28] explained in 2003 how federal agencies should incorporate the proportionality principle into their operations in connection with government services accessed on-line. The Guidance directs federal agencies to organize their on-line transactions and interactions with the public into four risk levels that reflect the degree of harm that could flow from an authentication failure and the likelihood of such harm. For example, according the Guidance, "Level 1" interactions require

---

sectors. It also recognizes that authentication requirements should be proportional to the risk they pose and that consumers should have choices about the authentication they use.

[27] CDT has outlined these and other Privacy Principles for Identity in the Digital Age. Version 1.4 of the principles, released in December 2007, can be found here: http://www.cdt.org/security/identity/20080108idprinciples.pdf. The privacy principles for identity that extend beyond proportionality and diversity are based on Principles of Fair Information Practices, and include specifying the purpose for the system being used, limiting the use and the retention period of personal information collected, giving individuals control and choice over identifiers needed to enroll in a system to the extent this is possible, providing notice about collection and use of personally identifiable information, security against misuse of the information provided, accountability, access and data quality.

[28] Joshua R. Bolten, Director, Office of Management and Budget, *E-Authentication Guidance for Federal Agencies,* December 16, 2003, http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00130 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.093

no authentication and include activities such as participating by name in an online discussion on the whitehouse.gov website. In contrast, a Level 3 interaction would require a much stronger level of authentication; examples might include a patent attorney submitting confidential patent information to the Patent and Trademark Office which, if improperly disclosed, would give competitors an advantage. The Guidance, of course, applies only to interactions with government systems, as is appropriate; many operators of critical systems in the private sector calready make similar risk assessments for their own unique systems and interactions and impose authentication requirements accordingly.

Under the diversity principle for privacy in identity management schemes, it is better to have multiple identification solutions, because use of a single identifier or credential creates a single target for privacy and security abuses. A single identifier also allows for multiple transactions and interactions to be tied to that identifier, permitting potentially invasive data surveillance. Instead, identification and enrollment options would function like keys on a key ring, with different identities for different purposes.[29] One model that holds great promise is the "user-centric" identity model, in which the user logs into a Web site through a third party identity provider, who passes on information at the user's request to the Web site in order to authenticate the user.

The White House Cyberspace Policy Review embraced the diversity and proportionality principles by calling for an array of interoperable identity management systems that would be used only for what it called "high value" activities, like certain smart grid functions, and then only on an opt-in basis. It also called for the federal government to build a security-based identity management vision and strategy for the nation, in collaboration with industry and civil liberties groups.

Recently, the General Services Administration took a major step in this direction by announcing three pilot programs for using user-centric identity management to improve access to government information while leveraging existing credentials for users. It has begun to set conditions that must be met by the identity credentials providers to ensure that identity providers are reliable and responsible.[30] Because the federal government is a leader in the provision of on-line services, this initiative could influence heavily the authentication and identification measures adopted by the private sector, including by critical infrastructure providers.

---

[29] *See*, Center for Democracy & Technology, *Privacy Principles for Identity in the Digital Age*, http://www.cdt.org/security/identity/20080108idprinciples.pdf, December 2007.

[30] http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf. CDT's recent analysis of this initiative and of the policy issues it raises can be found here: http://www.cdt.org/privacy/Issues_for_Responsible_UCI.pdf.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00131 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.094

Those who call for broad identity and authentication mandates across the Internet find no support in either the White House Cyberspace Policy Review or in the GSA initiative. We urge the Subcommittee to reject sweeping identity mandates and instead support and monitor more focused identity initiatives like the GSA's.

Conclusion

Policy makers should distinguish among different types of critical infrastructure when developing cybersecurity policy. One size does not fit all. Effective solutions will preserve the open, decentralized, user-controlled and innovative nature of the Internet and will tailor solutions to the systems that need protection.

Private network operators should monitor their own networks for evidence of intrusion and malicious code. Current law provides adequate authority for such monitoring, but may need to be clarified to ensure that "self protection" measures do not become backdoors for governmental monitoring of private networks. The Subcommittee should consider whether to craft a narrow exception from current surveillance statutes that would specifically permit communications service providers to share cyber attack information with each other and with the government to help defend other providers.

Likewise, the government should monitor its own networks for intrusion, but account for the chill to free speech and the right to petition the government that invasive monitoring could cause. Intrusion detection programs such as Einstein should be made more transparent.

Privacy and security are not a zero sum game. Measures intended to increase the security of communications and transactions – such as identity and authentication requirements – need not threaten privacy and indeed may enhance it if properly deployed.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00132 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.095

Statement for the Record

Philip Reitinger
Deputy Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States Senate
Committee on the Judiciary
Subcommittee on Terrorism and Homeland Security

Chairman Cardin, Ranking Member Kyl, and members of the Subcommittee, thank you for inviting me to appear before you today to discuss the work of the Department of Homeland Security (DHS) to improve the Nation's cybersecurity. Criminals and other adversaries attack critical U.S. systems every day, stealing valuable information, diverting funds to support criminal or terrorist activities, and compromising the online identities of Americans. The need to effectively prevent, protect against, and respond to these attacks is critical to the Nation's economic and national security, and both the public and private sectors have significant efforts underway that work toward preventing and disrupting cyber attacks against these assets.

Secretary Napolitano has designated me as the lead for DHS' broad set of cybersecurity responsibilities, both in my role as the Deputy Under Secretary of the National Protection and Programs Directorate (NPPD) and as the Director of the National Cyber Security Center. DHS is charged with protecting and defending both the federal government's civilian information systems and networks as well as collaborating with the private sector to ensure the resilience of privately owned infrastructure.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00133 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.096

To secure the federal executive branch's civilian networks and systems, DHS collaborates with its interagency partners. Currently, DHS is upgrading the federal government's capabilities to secure and defend against threats from individuals or organizations in cyberspace. In particular, the Department is focused on network defense activities geared toward defeating attacks from sophisticated high-level threat actors, that is, those who can potentially damage, cripple, and exploit these networks and systems. We are also working with federal civilian agencies to better secure their information systems and networks.

DHS also leads the federal government's work with the private sector to secure the Nation's critical communications and information technology infrastructure. This infrastructure—including the control systems that support the operations of electrical grids, manufacturing, health care, and banking—is largely owned and operated by the private sector. DHS collaborates with our private sector partners to ensure that resiliency, security, privacy, and other critical protections are built into these continually evolving infrastructures.

DHS has other cybersecurity mission areas beyond those of protecting federal and private sector networks and infrastructure. Specifically, the United States Secret Service investigates violations of U.S. laws relating to financial crimes and computer fraud and abuse. U.S. Immigration and Customs Enforcement's Cyber Crimes Center leads many trans-border criminal investigations into Internet-related crimes. And DHS' Science and Technology Directorate manages a full cybersecurity Research and Development lifecycle portfolio. In all this work, DHS has strong support from the White House, Congress, and our federal interagency partners, for our efforts to secure the systems, networks, and information on which we all rely in a manner

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00134 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.097

that enhances individual privacy and civil liberties, ensures that we remain true to our national values and operate within existing legal frameworks.

Given the interests of this Committee, I will turn my focus to two particular matters: our efforts to prevent and disrupt cyber attacks, and legal and privacy issues relating to cybersecurity.

Preventing and Disrupting Cyber Attacks

The Nation's electronic information infrastructure is vital to the functioning of government as well as to maintaining the Nation's economy and national security. This infrastructure comes under attack from a variety of sources, ranging from novice hackers to sophisticated groups that seek to gain or deny access to, disrupt, degrade, or destroy the systems and the data contained therein. As more of our critical infrastructure is connected to the Internet, malicious cyber activity will only increase and become more sophisticated and targeted, creating ever-greater potential for more severe consequences.

President Obama outlined the Administration's approach to cybersecurity in a public address in May. Under this plan, the Department of Homeland Security is leading efforts to secure federal executive branch civilian government networks. The Department, acting in its network defense capacity, treats sophisticated attacks from high-level threat actors as a key priority—we also work with critical infrastructure sectors to increase their cybersecurity. We maintain close ties with our intelligence and law enforcement partners, and we work to ensure that the overall level of preparedness is increasing in response to specific known and expected types of attacks from

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00135 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.098

any source. I would like to discuss four areas of work that support DHS' government and private sector cybersecurity missions. The first, cybersecurity protection, focuses primarily on government systems while the other three—incident response, collaboration and information sharing, and public awareness—focus on public/private partnership.

Cybersecurity Protection

The use of advanced technologies helps DHS improve its cybersecurity support to federal departments and agencies—for example, DHS' National Cybersecurity Division's (NCSD) within NPPD utilizes existing and currently deployed network flow monitoring and intrusion detection capabilities. DHS created the National Cybersecurity Protection Program to support the National Cybersecurity Protection System, operationally known as EINSTEIN. There are two versions of EINSTEIN at this time: EINSTEIN 1, a network flow monitoring system, and EINSTEIN 2, an intrusion detection system. In the future, DHS envisions deploying EINSTEIN 3, an intrusion prevention system, for federal executive branch civilian networks and systems. This more robust version of EINSTEIN would provide the federal government with an improved early warning and an enhanced situational awareness; the ability to automatically detect malicious activity; and the capability to prevent malicious intrusions before harm is done. In addition to this specific program, DHS has a variety of other initiatives under way to enhance the cybersecurity of civilian federal executive branch agencies and elements of the critical infrastructure. These include:

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00136 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.089

- Consolidating agencies' external Internet connections to reduce the number of entry points for potential outside threats;
- Developing a supply chain risk management framework to address security threats and vulnerabilities that could be introduced into hardware and software acquired by federal agencies;
- Establishing the Industrial Control Systems Cyber Emergency Response Team facility, which just opened earlier this month, to synchronize incident response activities related to attacks on control systems operating the Nation's critical infrastructure. It provides onsite forensic investigations and situational awareness in the form of actionable information, coordinates the responsible disclosure of vulnerabilities and mitigation solutions, and shares vulnerability information and threat analysis;
- Initiating an information-sharing pilot working with the Financial Services Information Sharing and Analysis Center to enhance threat information sharing with the financial services sector. The pilot is based on the good work that the Department of Defense has done with the Defense Industrial Base sector to increase actionable bi-directional information sharing.

Incident Response

The President's Cybersecurity Policy Review calls for *"a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident."* DHS has the lead for this initiative and is managing an interagency, state and local government, and private sector working group to develop a National Cyber Incident Response

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00137 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.100

Plan (NCIRP). This work will produce a clear delineation of roles and responsibilities in case of a major cyber incident and will update the Cyber Incident Response Annex to the National Response Framework created under Homeland Security Presidential Directive 5. Most importantly, we have launched this process with the private sector integrated from the very start, so that the end result will be an actionable response framework that will allow us to address a cyber incident as one Nation. In concert with the NCIRP, we are in the process of updating concepts of operations, standard operating procedures, and playbooks.

A key part of successful incident response is the ability to coordinate operations across multiple organizations. In this regard, DHS recently launched the National Cybersecurity and Communication Integration Center (NCCIC). As recommended by the President's National Security Telecommunications Advisory Committee and by other expert groups, the NCCIC co-locates the capabilities of various DHS cybersecurity and communications-related response organizations. Secretary Napolitano stated at the launch that the NCCIC will "serve as the central repository for cyber threat and incident reporting and provide improved operational situational awareness across the federal government, particularly across the civilian side of the federal government, as well as with the private sector." As it matures, we will incorporate additional capacity for state and local government participation onto the NCCIC operations floor. The NCCIC strengthens existing capabilities, and will continue to build trust by bringing together organizations whose common purpose is to protect shared cyber infrastructure. Early next year, we expect to exercise the NCCIC's operations, as well as the new response procedures defined in the NCIRP; further, during the Cyber Storm III exercise in September 2010, we will test these operations with substantial participation from the private sector.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00138 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.101

Collaboration and Information Sharing

Effective collaboration across government and industry has the potential to mitigate and even prevent a cyber attack. For example, when DHS's United States Computer Emergency Readiness Team (US-CERT) becomes aware of potential or occurring efforts to compromise government and/or private sector systems, it works with federal and industry partners to prevent or minimize disruptions to critical information infrastructures and protect the economy, government services, and the Nation's security. During Fiscal Year 2009, US-CERT produced more than 130 products to increase network and data security of public and private—both domestic and international—entities; sent over 30 alerts to the Government Forum of Incident Response and Security Teams (GFIRST), and posted more than 290 alerts to the US-CERT public-facing website.

As US-CERT upgrades its defensive technological and analytical capabilities, including EINSTEIN, the timeliness and quality of its products will improve. In addition to sending information to key stakeholders and the public, US-CERT is working to improve its operational collaboration with other federal agency responders. Last year, DHS established the Joint Agency Cyber Knowledge Exchange (JACKE), an interagency forum of federal agency cybersecurity incident responders. The JACKE provides a venue for customer feedback to US-CERT and recommendations to improve the practices of federal security operation centers. Fifteen agencies are participating, and the next step is to expand participation to include all 26 major departments and agencies. We believe efforts like JACKE will help US-CERT better understand the views of

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00139 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.102

its customers, thereby improving its products and services. This process will also better inform the products we share with the private sector and the public.

Finally, earlier this year, DHS hosted an industry day to highlight the need for private industry to become more involved in developing comprehensive, game-changing, innovative solutions that improve and expand upon our current capabilities. As a follow-up, DHS released a classified request for information to the private sector to identify prospective private sector technical, end-to-end solutions for protecting the federal cyber domain.

Public Awareness

As stated in the President's Cyberspace Policy Review, *"People cannot value security without first understanding how much is at risk. Therefore, the Federal government should initiate a national public awareness and education campaign."* In that spirit, DHS reached out to the public broadly in October, during the sixth annual Cybersecurity Awareness Month, which focused this year on shared responsibility. During the month, Secretary Napolitano delivered three public speeches on cybersecurity and participated in several other outreach efforts, including meetings in Silicon Valley with industry leaders and two public web chats broadcast on www.dhs.gov. In support of these efforts, other DHS personnel delivered nearly 60 cybersecurity speeches in October, promoting shared responsibility for cybersecurity among all stakeholders, including the creation of a culture of cybersecurity in organizations. As in past years, DHS worked with stakeholder organizations such as the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center to expand our reach into the private

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00140 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.103

sector. We will continue this important work with stakeholders and partners in the months ahead.

Legal and Privacy Issues

Efforts to secure cyberspace are accompanied by complex, interrelated, and international legal and privacy issues. Let me turn first to general legal issues, and then more specifically to privacy. As the President's Cyberspace Policy Review notes:

"Law applicable to information and communications networks is a complex patchwork of Constitutional, domestic, foreign, and international laws that shapes viable policy options...As traditional telecommunications and Internet-type networks continue to converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity, law and policy should continue to seek an integrated approach that combines the benefits of flexibility and diversity of applications and services with the protection of civil liberties, privacy rights, public safety, and national and economic security interests...Policy decisions will necessarily be shaped and bounded by the legal framework in which they are made, and policy consideration may help identify gaps and challenges in current laws and inform necessary developments in the law. That process may prompt proposals for a new legislative framework to rationalize the patchwork ...or the applications of new interpretations of existing laws in ways to meet technological evolution and policy goals, consistent with U.S. Constitutional principles."

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00141 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.104

DHS works closely with DOJ and other agencies to resolve specific legal issues around particular activities. For example, as the Subcommittee is aware, the DOJ Office of Legal Counsel has issued opinions regarding the EINSTEIN 2 program and affirming its compliance with the Fourth Amendment to the Constitution, the Wiretap Act, the Foreign Intelligence Surveillance Act, the Stored Communications Act, 18 U.S.C. § 270(a)(1), the pen register, and trap and trace provisions of chapter 206 of title 18, United States Code.[1] We will continue to work closely with DOJ to proactively address these important legal issues as we improve our defensive cybersecurity capabilities.

In this regard, the Comprehensive National Cybersecurity Initiative (CNCI) effort operates under executive guidance that all actions pursuant to this initiative will be implemented in a manner that ensures protection of privacy rights and other legal rights of Americans. The Secretary of Homeland Security is the lead official for the national effort to protect, defend, and reduce vulnerabilities of federal executive branch civilian systems. Accordingly, the specific privacy provisions[2] of section 222 of the Homeland Security Act apply to all DHS cybersecurity and CNCI activities.

Compliance with privacy statutes is critical, but even more can be done: increased cybersecurity creates an opportunity to enhance privacy and civil liberties. Whether it is by lowering the incidence of identity theft through stronger authentication regimes, or by protecting anonymity

[1] *See* Memorandum Opinion for an Associate Deputy Attorney General, Legality Of Intrusion-Detection System To Protect Unclassified Computer Networks In The Executive Branch (August 14, 2009); Memorandum Opinion for the Counsel to the President, Legal Issues Relating To The Testing, Use, And Deployment Of An Intrusion-Detection System (Einstein 2.0) To Protect Unclassified Computer Networks In The Executive Branch (January 9, 2009), both available at http://www.justice.gov/olc/allopinions.htm.

[2] In particular, that section charges the Department's Chief Privacy Officer with "assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00142 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.105

on government websites where free speech or privacy considerations are predominant, the U.S. government must lead the way, in cooperation with our state and local partners and the private sector.

Accordingly, DHS and its partners have taken decisive steps as we add, upgrade, and build upon existing defensive cybersecurity capabilities. DHS has, and will continue to incorporate privacy rights and civil liberties protections into the operating procedures and the architectural engineering development and deployment schedule for each iteration of EINSTEIN. As an added layer of protection, DHS has created an Oversight and Compliance Officer position within the Office of the Assistant Secretary for Cybersecurity and Communications, whose primary function is the monitoring and oversight of the EINSTEIN program. Additionally, DHS's Chief Privacy Officer is part of the development team and is reviewing all components of the EINSTEIN system to determine which elements require a privacy impact assessment (PIA). The Privacy Office will continue to perform thorough privacy analysis and publish as much of the privacy analysis as possible, consistent with security classification.[3] More broadly, the DHS Privacy Office provides privacy training and oversight to US-CERT personnel and the operators of the EINSTEIN system. Furthermore, the DHS Office for Civil Rights and Civil Liberties is participating in the design, planning, and execution of the EINSTEIN program, providing proactive advice on how enhanced cybersecurity efforts may be conducted in a manner consistent with civil rights and civil liberties.

With respect to identity management, the President's Cyberspace Policy Review included the building of "*a cybersecurity-based identity management vision and strategy that addresses*

[3] The PIAs for EINSTEIN 1 and EINSTEIN 2 are publicly available on http://www.dhs.gov/.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00143 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.106

privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation" as a near-term priority. The objective is a system that is voluntary, secure, affordable, easy-to-use, and privacy-enhancing. That system should also accommodate a variety of technologies and governance mechanisms, working in an interoperable, decentralized manner. Building that vision and strategy, and including privacy into the design from the beginning, will encourage broad deployment of mechanisms that will reduce identity theft and the theft of other personally identifiable information, and empower the American people to make effective decisions to protect their safety, security and privacy.

Conclusion

In closing, I would like to emphasize that developing and implementing the technical solutions necessary to secure the federal executive branch civilian networks and systems is complicated and requires sophisticated technology. At the same time, these solutions must ensure the continued protection of civil rights, civil liberties, and privacy protections. The President and DHS are committed to transparency and the responsible disclosure of information. We look forward to continuing to work with this Subcommittee and others to ensure that the American people have the information needed to understand the criticality of the systems we protect and the measures in place to mitigate cybersecurity risks.

I appreciate the opportunity to discuss the Department's efforts in advancing our cybersecurity posture and increasing the security of federal networks. I will be happy to answer any questions from the Subcommittee.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00144 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.107

Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace

Testimony of the
National Security Agency's Information Assurance Director
Before the Senate Committee on the Judiciary's Subcommittee
On Terrorism and Homeland Security

Statement for the Record

November 17, 2009

Good morning, Chairman Cardin, Ranking Member Kyl, and distinguished members of the Subcommittee. My name is Richard C. Schaeffer, Jr., and I am the National Security Agency's (NSA) Information Assurance Director. I appreciate the opportunity to be here today to talk briefly about the NSA's information assurance mission and its relationship to the work of the Department of Homeland Security and others concerned with helping operators of crucial information systems protect and defend their data, systems and networks from hostile acts or other disruptive events.

I would also like to thank the Chairman and the other members of the Subcommittee for their continued interest in, and attention to, this issue. Each day, ever more data and functions that are vital to the nation are consigned to digital systems and complex, inter-dependent networks. There are no "silver bullets" when it comes to cybersecurity, but over time, increased awareness of cybersecurity issues, new standards, better education, expanded information sharing, more uniform practices, and improved technology can and does make a meaningful difference.

The NSA information assurance mission focuses on protecting what National Security Directive 42 defines as "national security systems", systems that process, store, and transmit classified information or are otherwise critical to military or intelligence activities. Historically, much of our work has been sponsored by and tailored for the Department of Defense. Today, national security systems are heavily dependent on commercial products and infrastructure, or interconnect with systems that are. This creates new and significant common ground between defense and broader U.S. Government and homeland security needs. More and more, we find that protecting national security systems demands teaming with public and private institutions to raise the information assurance level of products and services more broadly. If done correctly, this is a win-win situation that benefits the whole spectrum of information technology (IT) users, from warfighters and policymakers, to federal, state, local and tribal governments, to the operators of critical infrastructure and the nation's major arteries of commerce.

This convergence of interests has been underway for some time and we can already point to significant examples of the kind of fruitful collaboration it inspires. For instance, the NSA and the National Institute of Standards and Technology (NIST) have been working together for several years to characterize cyber vulnerabilities, threats, and countermeasures, to provide practical cryptographic and cyber security guidance to both

61662.108

IT suppliers and consumers. Among other things, we've compiled and published security checklists for hardening computers against a variety of threats; we've shaped and promoted standards that enable information about computer vulnerabilities to be more easily cataloged and exchanged and, ultimately, the vulnerabilities themselves to be automatically patched; and we've begun studying how to extend our joint vulnerability management efforts to directly support compliance programs such as those associated with the Federal Information Security Management Act. All of this is unclassified and advances cyber security in general, from national security and other government networks to critical infrastructure and other commercial or private systems.

The NSA partners similarly with the Department of Homeland Security (DHS). Earlier this year we together proudly announced the designation of 29 additional U.S. colleges and universities as National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) and/or Information Assurance Research (CAE-R). This brings the number of institutions participating in this highly regarded program to 106, located in 37 states, the District of Columbia and the Commonwealth of Puerto Rico.

Universities designated as National Centers of Academic Excellence in Information Assurance are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs. Graduates from Information Assurance programs at CAE institutions become a critical part of the core of professional cyber security experts protecting national security information systems, commercial networks and critical information infrastructure. These professionals are helping to meet the increasingly urgent needs of the U.S. government, industry, academia and research.

The NSA/DHS partnership was formed in 2004 in response to the ***President's National Strategy to Secure Cyberspace*** of 2003. The CAE-R program was added in 2007 to encourage universities and students to pursue research, development and innovation in Information Assurance (cyber security). The program originally created by this partnership has continued to grow and become even more relevant and critical to U.S. national security today.

NSA and DHS collaborate daily, cooperating on investigations and forensic analysis of cyber incidents and malicious software, and together we look for and mitigate the vulnerabilities in various technologies that would render them susceptible to similar attacks. We each bring to these efforts complementary experience, insight, and expertise based on the different problem sets and user communities on which we concentrate, and we each then carry back to those communities the dividends of our combined wisdom and resources.

Key to the Nation's Cybersecurity efforts is the Public-Private Sector relationship, which has been actively embraced by the Federal Government, industry and academia. This trusting relationship includes...and is based upon...the common goal of improving cybersecurity, the sharing of information, and collaborative research, development and innovation. A recent example of this continuing and close collaboration is last month's 5th Annual Security Automation Conference at the Baltimore Convention Center, co-

hosted by NSA, NIST, DHS and the Defense Information Systems Agency (DISA). In fact, it brought together for several days nearly 1,000 representatives from the public and private sectors and demonstrated the benefits of automation and standardization of vulnerability management, security management, and security compliance.

In the past, proprietary technologies and methodologies have made it difficult to identify, remediate, and report on vulnerabilities in mission critical systems and data. Over the past few years, the Information Assurance Directorate at NSA has played a leadership role in developing security automation standards and fostering the adoption of security automation and security baselines across the DoD. These standards include the Security Content Automation Protocol (SCAP), Common Vulnerability Enumeration (CVE) and the Federal Desktop Core Configuration (FDCC). This year's conference showcased numerous SCAP-validated tools designed to simplify security management in DoD systems, increase interoperability in products, and reduce the cost of vulnerability management for our DoD customers. Established by NIST five years ago with an attendance of less than 50 people, the conference is now jointly sponsored by the four agencies, mentioned above. The benefits reach throughout industry as evidenced by the major industry vendors who participated.

NSA works directly and indirectly with vendors across the information technology and security community to develop and distribute configuration guidance for a wide variety of software and hardware products. We engage vendor products through deep technical analysis of vulnerabilities within the technology and from what we learn by conducting operations to find vulnerabilities in DoD systems. NSA keeps abreast of new vulnerabilities in these technologies and strives to provide customers and the IT community with the best possible security options for the most widely used products across the IT community and the DoD.

NSA, in partnership with NIST, Mitre, Symantec, McAfee, Intel, and many other security vendors, is actively encouraging the IT industry to utilize SCAP Protocols to provide managers with a greater understanding of risks, real data upon which to make management decisions, and the ability to give technical direction regarding the security of their networks and applications. SCAP is a group of standards that enable organizations to automate compliance, manage vulnerabilities, perform security measurement, and perform a host of other Asset, Vulnerability, and Configuration Management related tasks. Further, NSA's technical expertise and operational knowledge in cryptography improves hash standards for commercial industry through NIST's Hash competition. NSA brings its experience to the NIST decision making process, which selects high assurance hashes that commercial industry uses to secure things such as the storage of passwords and to provide software integrity checks.

Starting in 2005, NSA started working with DISA, DHS, NIST, Microsoft, Army, Navy, Marines, and Air Force to build consensus on common security configurations for Microsoft Operating systems such as XP, Vista, Internet Explorer, and firewalls. These common configurations ensured improved security, performance, power management, feature compatibility, and usability configuration settings for DoD purchased systems.

The Air Force utilized these settings to develop the Federal Desktop Core Configuration (FDCC) for all Air Force purchased operating systems. Working with vendors to pre-configure, pre-install, and pre-test configurations of their OS helps reduce purchase costs, improve security, and enables improved vulnerability and situational awareness. This FDCC work, ultimately saving millions of dollars for DoD, led to OMB adoption of the Windows/IE configurations as Federal-wide standards. NSA and the configuration working groups are now engaging additional vendors such as Apple, Sun, and RedHat to develop secure baselines for their products.

The recent announcement by Microsoft of the release of Windows 7 was quickly followed by the release of the security configuration guide for this state of the art operating system. Working in partnership with Microsoft and elements of the DoD, NSA leveraged our unique expertise and operational knowledge of system threats and vulnerabilities to enhance Microsoft's operating system security guide without constraining the user's ability to perform their everyday tasks, whether those tasks are being performed in the public or private sector. All this was done in coordination with the product release, not months or years later during the product lifecycle. This will improve the adoption of the security advice, as it can be implemented during installation and then later managed through the emerging SCAP standards.

As LTG Alexander, NSA's Director, stated clearly in his address to the RSA Security Conference this past April, Cybersecurity is a big job and it's going to take a team to do it. We'll bring our technical expertise and working with many others in the public and private sector we'll comprise the "team" the nation needs to address this challenge.

This concludes my remarks. I would be pleased to answer questions from you and others members of the Subcommittee.

United States Government Accountability Office

GAO

Statement for the Record
To the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, November 17, 2009

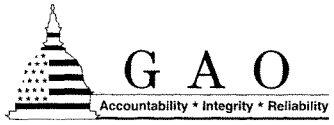
CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues



GAO-10-230T

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00149 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.112

Abbreviations

DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
NASA	National Aeronautics and Space Administration
OMB	Office of Management and Budget
TVA	Tennessee Valley Authority
US-CERT	United States Computer Emergency Readiness Team

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

November 17, 2009

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-10-230T, a statement to the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Why GAO Did This Study

Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the federal government. In recent months, federal officials have cited the continued efforts of foreign nations and criminals to target government and private sector networks; terrorist groups have expressed a desire to use cyber attacks to target the United States; and press accounts have reported attacks on the Web sites of government agencies. The ever-increasing dependence of federal agencies on computerized systems to carry out essential, everyday operations can make them vulnerable to an array of cyber-based risks. Thus it is increasingly important for the federal government to have effective information security controls in place to safeguard its systems and the information they contain.

GAO was asked to provide a statement describing (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies at federal agencies that make these systems and infrastructures vulnerable to cyber threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, GAO relied on its previously published work in this area.

View GAO-10-230T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can be unintentional or intentional, targeted or non-targeted, and can come from a variety of sources, including criminals, terrorists, and adversarial foreign nations, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and cyber attackers can more easily preserve their anonymity. Further, the growing interconnectivity between information systems, the Internet, and other infrastructure presents increasing opportunities for such attacks. In addition, reports of security incidents from federal agencies are on the rise, increasing by over 200 percent from fiscal year 2006 to fiscal year 2008.

Compounding the growing number and kinds of threats, GAO—along with agencies and their inspectors general—has identified significant weaknesses in the security controls on federal information systems, resulting in pervasive vulnerabilities. These include deficiencies in the security of financial systems and information and vulnerabilities in other critical federal information systems. GAO has identified weaknesses in all major categories of information security controls at federal agencies. For example, in fiscal year 2008, weaknesses were reported in such controls at 23 of 24 major agencies. Specifically, agencies did not consistently authenticate users to prevent unauthorized access to systems; apply encryption to protect sensitive data; and log, audit, and monitor security-relevant events, among other actions. An underlying cause of these weaknesses is agencies' failure to fully or effectively implement information security programs, which entails assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of security controls, and implementing appropriate remedial actions.

Multiple opportunities exist to enhance cybersecurity. In light of weaknesses in agencies' information security controls, GAO and inspectors general have made hundreds of recommendations to improve security, many of which agencies are implementing. In addition, the White House and the Office of Management and Budget, collaborating with other agencies, have launched several initiatives aimed at improving aspects of federal cybersecurity. The Department of Homeland Security, which plays a key role in coordinating cybersecurity activities, also needs to fulfill its responsibilities, such as developing capabilities for protecting cyber-reliant critical infrastructures and implementing lessons learned from a major cyber simulation exercise. Finally, a panel of experts convened by GAO made several recommendations for improving the nation's cybersecurity strategy. Realizing these opportunities for improvement can help ensure that the federal government's systems, information, and critical cyber-reliant infrastructure are effectively protected.

United States Government Accountability Office

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00151 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.114

Chairman Cardin and Members of the Subcommittee:

Thank you for the opportunity to submit this statement for the record for today's hearing on public and private sector efforts to prevent and disrupt terrorist cyber attacks against computer networks.

Pervasive and sustained cyber attacks against the United States continue to pose a potentially devastating impact on federal systems and operations. In February 2009, the Director of National Intelligence testified that foreign nations and criminals had targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups had expressed a desire to use cyber attacks as a means to target the United States.[1] As recently as July 2009, press accounts reported that a widespread and coordinated attack over the course of several days targeted Web sites operated by major government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of government information. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

In this statement we will describe (1) cyber threats to federal information systems and cyber-based critical infrastructures, (2) control deficiencies that make these systems and infrastructures vulnerable to those threats, and (3) opportunities that exist for improving federal cybersecurity. In preparing this statement, we relied on our previous reports on federal information security. These reports contain detailed overviews of the scope and methodology we used. The work on which this statement 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 evidence to provide

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

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00152 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.115

a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided 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. Examples of such risks include the following:

- 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.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00153 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.116

- 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 that these threats can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources.[2] 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. The Federal Bureau of Investigation has identified multiple sources of threats to our 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 and types of individuals that are considered to be key sources of cyber threats to our nation's information systems and cyber infrastructures.

[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.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00154 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.117

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 potential 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 have been less developed in their computer network capabilities than other adversaries. 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 the Director of National 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,[4] the 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.

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

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00155 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.118

- 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.

The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. 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. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. For example, the Director of National Intelligence 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 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

Consistent with 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.

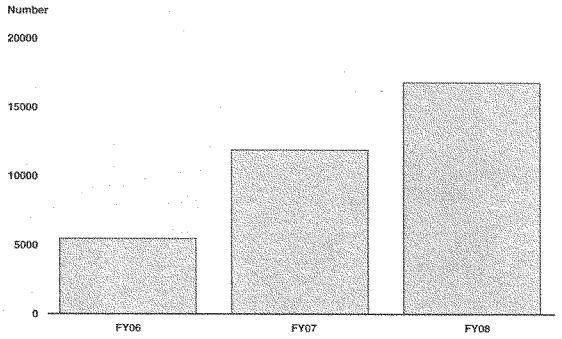
When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00156 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.119

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.

The three most prevalent types of incidents reported to US-CERT during fiscal years 2006 through 2008 were unauthorized access (where an individual gains logical or physical access to a system without permission), improper usage (a violation of acceptable computing use policies), and investigation (unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00157 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.120

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.

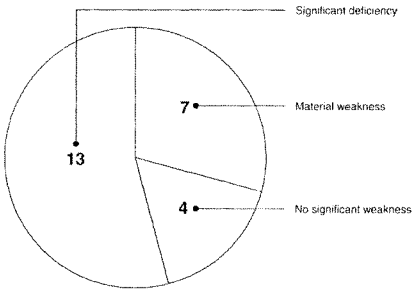
In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information system controls over financial systems and information were either a significant deficiency or a material weakness for financial statement reporting (see fig. 2).[5]

[5]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.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00158 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.121

Figure 2: 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[6] that, although the Los Alamos National Laboratory—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. In addition, in May 2008[7] 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. Similarly, in

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

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

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00159 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.122

October 2009[8] we reported that the National Aeronautics and Space Administration (NASA)—the civilian agency that oversees U.S. aeronautical and space activities—had not always implemented appropriate controls to sufficiently protect the confidentiality, integrity, and availability of the information and systems supporting its mission directorates.

Weaknesses Persist in All Major Categories of Controls

Over the last several years, most agencies have not implemented controls sufficiently to prevent, limit, or detect unauthorized access to computer networks, systems, or information. Our analysis of inspectors general, agency, and our own reports determined 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.

An underlying cause of 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 (FISMA),[9] is intended to

[8] GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009).

[9] 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).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00160 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.123

provide a framework and continuing cycle of activities, including 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.

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,[10] a designation we have made in each report since 1997.

Opportunities Exist for Enhancing Federal Cybersecurity

Over the past several years, we and inspectors general 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 weaknesses 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. Agencies have implemented or are in the process of implementing many of our recommendations.

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

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00161 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.124

In June 2009[11] we proposed a list of suggested actions that could improve FISMA and its associated implementing guidance, including (1) clarifying requirements for testing and evaluating security controls; (2) requiring agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program; (3) enhancing independent annual evaluations; and (4) strengthening annual reporting mechanisms.

In addition, the White House, OMB, and certain federal agencies have undertaken 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's (DHS) and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[12] While details of these initiatives have not been made public, the Director of National Intelligence stated that they include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public-private partnerships.[13]
- *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 computer security awareness training and FISMA reporting.

[11] GAO, *Federal Information Security Issues*, GAO-09-817R (Washington, D.C.: June 30, 2009).

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

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

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00162 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.125

- *Federal Desktop Core Configuration:* For this initiative, OMB directed agencies that have Windows XP and/or Windows Vista operating systems deployed to adopt the security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs.
- *Einstein:* This is a computer network intrusion detection system that analyzes network flow information from participating federal agencies. The system is to provide a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks.
- *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.

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

DHS Needs to Fully Satisfy Its Cybersecurity Responsibilities

Federal law and policy[14] establish DHS as the focal point for efforts to protect our nation's computer-reliant critical infrastructures[15]—a practice known as cyber critical infrastructure protection, or cyber CIP. We have reported since 2005 that DHS has yet to fully satisfy its

[14] These include The Homeland Security Act of 2002, Homeland Security Presidential Directive-7, and the *National Strategy to Secure Cyberspace*.

[15] Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: agriculture and food; banking and finance; chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; government facilities; information technology; national monuments and icons; nuclear reactors, materials and waste; postal and shipping; public health and health care; transportation systems; and water.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00163 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.126

key responsibilities for protecting these critical infrastructures. Our reports included recommendations that are essential for DHS to address in order to fully implement its responsibilities. We summarized these recommendations into key areas listed in table 2.

Table 2: Key Cybersecurity Areas Identified by GAO

1. Bolstering cyber analysis and warning capabilities
2. Improving cybersecurity of infrastructure control systems
3. Strengthening DHS's ability to help recover from Internet disruptions
4. Reducing organizational inefficiencies
5. Completing actions identified during cyber exercises
6. Developing sector-specific plans that fully address all of the cyber-related criteria
7. Securing internal information systems

Source: GAO

DHS has since developed and implemented certain capabilities to satisfy aspects of its responsibilities, but the department still has not fully implemented our recommendations, and thus further action needs to be taken to address these areas. For example, in July 2008, we reported[16] that DHS's US-CERT did not fully address 15 key attributes of cyber analysis and warning capabilities related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations.

Similarly, in September 2008, we reported that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned

[16] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00164 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.127

from these efforts.[17] However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the department had identified 16 activities as ongoing and 7 as planned for the future.[18] Consequently, we recommended that DHS schedule and complete all of the corrective activities identified in order to strengthen coordination between public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation. Since that time, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

Improving the National Cybersecurity Strategy

Because the threats to federal information systems and critical infrastructure have persisted and grown, efforts have recently been undertaken by the executive branch to review the nation's cybersecurity strategy. As we previously stated, in January 2008 the Comprehensive National Cybersecurity Initiative was established with its primary aim to improve federal agencies' efforts to protect against intrusion attempts and anticipate future threats. In February 2009, President Obama directed the National Security Council and Homeland Security Council to conduct a comprehensive review to assess the United States' cybersecurity-related policies and structures. The resulting report, *"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,"* recommended, among other things, appointing an official in the White House to coordinate the nation's cybersecurity policies and activities, creating a new national cybersecurity strategy, and developing a framework for cyber research and development.[19] We recently initiated a review to assess the progress

[17] GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

[18] At that time, DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

[19] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00165 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.128

made by the executive branch in implementing the policy's recommendations.

We also testified in March 2009 on needed improvements to the nation's cybersecurity strategy.[39] In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 3.

Table 3: Key Strategy Improvement Identified by Cybersecurity Experts

1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2. Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3. Establish a governance structure for strategy implementation.
4. Publicize and raise awareness about the seriousness of the cybersecurity problem.
5. Create an accountable, operational cybersecurity organization.
6. Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7. Bolster public-private partnerships through an improved value proposition and use of incentives.
8. Focus greater attention on addressing the global aspects of cyberspace.
9. Improve law enforcement efforts to address malicious activities in cyberspace.
10. Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11. Increase the cadre of cybersecurity professionals.
12. Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research and experience in this area. Until they are addressed, our

[39] GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: March 10, 2009).

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00166 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.129

nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

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. To help in meeting these threats, opportunities exist to improve information security throughout the federal government. The White House, OMB, and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. In addition, the prompt and effective implementation of the hundreds of recommendations by us and by agency inspectors general to mitigate information security control deficiencies and fully implement agencywide security programs would also strengthen the protection of federal information systems, as would efforts by DHS to develop better capabilities to meets its responsibilities, and the implementation of recommended improvements to the national cybersecurity strategy. Until agencies fully and effectively implement these recommendations, federal information and systems will remain vulnerable.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov, or David A. Powner at (202) 512-9286 or pownerd@gao.gov. Other key contributors to this statement include John de Ferrari (Assistant Director), Matthew Grote, Nick Marinos, and Lee McCracken.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00167 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.130

Related GAO Products

Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks. GAO-10-4. Washington, D.C.: October 15, 2009.

Information Security: Concerted Effort Needed to Improve Federal Performance Measures. GAO-09-617. Washington, D.C.: September 14, 2009.

Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses. GAO-09-546. Washington, D.C.: July 17, 2009.

Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information. GAO-09-835T. Washington, D.C.: June 25, 2009.

Privacy and Security: Food and Drug Administration Faces Challenges in Establishing Protections for Its Postmarket Risk Analysis System. GAO-09-355. Washington, D.C.: June 1, 2009.

Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks. GAO-09-292. Washington, D.C.: May 13, 2009.

Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. GAO-09-661T. Washington, D.C.: May 5, 2009.

Freedom of Information Act: DHS Has Taken Steps to Enhance Its Program, but Opportunities Exist to Improve Efficiency and Cost-Effectiveness. GAO-09-260. Washington, D.C.: March 20, 2009.

Information Security: Securities and Exchange Commission Needs to Consistently Implement Effective Controls. GAO-09-203. Washington, D.C.: March 16, 2009.

National Cyber Security Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture. GAO-09-432T. Washington, D.C.: March 10, 2009.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00168 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.131

Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data. GAO-09-195. Washington, D.C.: January 30, 2009.

Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS. GAO-09-136. Washington, D.C.: January 9, 2009.

Nuclear Security: Los Alamos National Laboratory Faces Challenges in Sustaining Physical and Cyber Security Improvements. GAO-08-1180T. Washington, D.C.: September 25, 2008.

Critical Infrastructure Protection: DHS Needs to Better Address Its Cyber Security Responsibilities. GAO-08-1157T. Washington, D.C.: September 16, 2008.

Critical Infrastructure Protection: DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise. GAO-08-825. Washington, D.C.: September 9, 2008.

Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network. GAO-08-1001. Washington, D.C.: September 9, 2008.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. GAO-08-588. Washington, D.C.: July 31, 2008.

Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains. GAO-08-525. Washington, D.C.: June 27, 2008.

Information Security: FDIC Sustains Progress but Needs to Improve Configuration Management of Key Financial Systems. GAO-08-564. Washington, D.C.: May 30, 2008.

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

Information Security: TVA Needs to Enhance Security of Critical Infrastructure Control Systems and Networks. GAO-08-775T. Washington, D.C.: May 21, 2008.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00169 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.132

Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist. GAO-08-571T. Washington, D.C.: March 12, 2008.

Information Security: Securities and Exchange Commission Needs to Continue to Improve Its Program. GAO-08-280. Washington, D.C.: February 29, 2008.

Information Security: Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies. GAO-08-496T. Washington, D.C.: February 14, 2008.

Information Security: Protecting Personally Identifiable Information. GAO-08-343. Washington, D.C.: January 25, 2008.

Information Security: IRS Needs to Address Pervasive Weaknesses. GAO-08-211. Washington, D.C.: January 8, 2008.

Veterans Affairs: Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and Strengthening Information Security. GAO-07-1264T. Washington, D.C.: September 26, 2007.

Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. GAO-07-1036. Washington, D.C.: September 10, 2007.

Information Security: Sustained Management Commitment and Oversight Are Vital to Resolving Long-standing Weaknesses at the Department of Veterans Affairs. GAO-07-1019. Washington, D.C.: September 7, 2007.

Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements. GAO-07-528. Washington, D.C.: August 31, 2007.

Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses. GAO-07-837. Washington, D.C.: July 27, 2007.

Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program. GAO-07-870. Washington, D.C.: July 13, 2007.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00170 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.133

Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program. GAO-07-1003T. Washington, D.C.: June 20, 2007.

Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk. GAO-07-935T. Washington, D.C.: June 7, 2007.

Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program. GAO-07-351. Washington, D.C.: May 18, 2007.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00171 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC
61662.134

Preventing Terrorist Attacks, Countering Cyber Intrusions, and Protecting Privacy in Cyberspace

Testimony before the Subcommittee on Terrorism and Homeland Security

United States Senate

By

Larry M. Wortzel
Vice Chairman
U.S.-China Economic and Security Review Commission

November 17, 2009

Dirksen Senate Office Building

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00172 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.135

Chairman Cardin, Ranking Member Kyl, thank you for giving me the opportunity to testify today on cyber threats, security, preventing terrorist acts, and protecting the privacy of Americans.

Our nation's critical infrastructure, economy, defense information, and citizens are threatened by hackers, terrorists, and hostile foreign intelligence services. Preventing computer network penetration and pursuing those who attack us while at the same time preserving civil liberties and privacy is a challenge. Our intelligence and law enforcement agencies have been successful in preventing terrorist attacks and detecting espionage because of laws such as the Foreign Intelligence and Surveillance Act and the PATRIOT Act. With more of such legislation, and with careful oversight and attention from Congress and the White House, our intelligence agencies and law enforcement authorities can accomplish much in protecting America's computer networks.

In my remarks, I'll make reference to a report the U.S.-China Economic and Security Review Commission recently released on China's capability to conduct cyber warfare and to penetrate and exploit computer networks.[1] The report's findings are relevant to the challenge of securing critical infrastructure and to preventing cyber attacks. And the lessons learned by preventing intrusions from China can be applied to all other forms of intrusions, including those attempted by terrorist groups.

In addition to discussing the Commission's findings about cyber security and our recommendations to Congress, I will provide my personal views, informed by my experience as a U.S. Army intelligence officer and by my research while employed at The Heritage Foundation.[2]

We can do better in some areas. I do not believe that the Computer Fraud and Abuse Act, even as amended by the PATRIOT Act, is yet sufficient to address certain critical issues. This includes the right of private response to computer penetrations, such as cyber

---

[1] See Bryan Krekel et al, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," *U.S.-China Economic and Security Review Commission*, October 2009. *http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf*.

[2] See Larry M. Wortzel and Michael Scardaville, "The New Agenda for Homeland Security," *Heritage Foundation Executive Memorandum #779,* September 28, 2001; Wortzel, "Let Congress Do its Job and Protect the American People," *Heritage Foundation Web Memo #101,* May 28, 2002; Wortzel, "Creating an Intelligent Department of Homeland Security," *Heritage Foundation Executive Memorandum #828,* August 23, 2002; Wortzel, "Americans Do Not Need a New Domestic Spy Agency to Improve Intelligence and Homeland Security," *Heritage Foundation Executive Memorandum #848,* January 10, 20003; Wortzel, "Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security," *Heritage Lecture #878;* May 7, 2003; Edwin Meese III, Larry M. Wortzel, Peter Brookes, and James Jay Carafano, "What a Comprehensive Intelligence Bill Should Contain," *Heritage Foundation Backgrounder #1799,* September 24, 2004; also relevant is James Jay Carafano, Todd Gaziano and Alane Kochems, "Domestic Surveillance: Dual Priorities, National Security and Civil Liberties Must be Met," *Heritage Foundation Web Memo #950,* December 21, 2005. All of these documents can be found at *www.heritage.org*; see also Larry M. Wortzel, "China's Cyber Offensive: And how the U.S. Can Respond," *The Wall Street Journal,* November 1, 2009 *http://online.wsj.com/article/SB10001424052748703399204574084138499779406.html*.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00173 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.136

counterattacks, by our government or private individuals or companies in retaliation for cyber intrusions.

As our Commission's report documents, there have been significant penetrations of our critical infrastructure, our defense contractors, and government cyber networks, including those of the Department of Defense. The Commission recommended that Congress respond by evaluating the effectiveness and the resources available for law enforcement and the Intelligence Community. Among the most important objectives should be developing reliable attribution techniques to determine the origin of computer exploitations and attacks. The Commission also recommended that Congress urge the Obama administration to develop measures to deter malicious Chinese cyber activity.

In a recent editorial, I pointed out that government and private industry are still in a reactive posture to cyber intrusions and cyber espionage.[3] As yet, there is no fully coordinated government and industry response. President Obama made a good start with the 60-day cyber review earlier this year, but there still is no cyber security coordinator at the White House, as recommended by the White House review. Efforts to coordinate standards and policies across government and in the private sector appear stalled without the support of senior leadership in the National Security Council.

That said, I think President Obama was wise to incorporate the Homeland Security Council Staff into the National Security Council. The National Security Act of 1947 is a fine model. With proper staffing in the White House and attention from the National Security Advisor, a unified, well-led effort can bring together the agencies of the government and coordinate cyber security with allies and private industry. Also, creating the U.S. Cyber Command is an outstanding initiative within the Department of Defense.

There is still debate about what agency should lead cyber efforts and set standards. The Department of Homeland Security can help to coordinate these with state and local governments as well as private industry.

I believe the lead agency, however, should be the National Security Agency (NSA). NSA has a strong institutional culture of adherence to the Foreign Intelligence and Surveillance Act. Its personnel, like all the members of the intelligence community, are trained to protect the privacy and rights of American persons. No agency has the decades of experience the National Security Agency has in conducting operations in the electronic and cyber realms; its personnel are skilled and superbly trained; it has broad international contacts with allies and friendly governments; it has wide contacts in the private sector; and it has a cadre of highly skilled linguists able to work in the languages associated with the origin of the foreign intrusions.

{End of Oral Testimony, written submission continues below}

[3] Larry M. Wortzel, "China's Cyber Offensive: And how the U.S. Can Respond," *The Wall Street Journal*, November 1, 2009. See also Larry M. Wortzel, "China Goes on the Cyber-Offensive," *Far Eastern Economic Review*, January/February 2009, www.feer.com.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00174 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.137

Most of my recent work has been on China. Therefore as I frame the severity of the cyber threats we face, I am going highlight China as a substantial part of the problem. I recognize, however, that the concerns of this Committee extend far beyond only the malicious activities of one country. But the threat to our computer networks posed by the Chinese military, government, and individual hackers parallels the danger America faces from other countries and from terrorist organizations.

Reliable statistics about the quantity of cyber attacks against U.S. information systems are difficult to compile. But by most measures, attacks are on the rise. Take recent data from the Department of Defense (DoD) as an example: from 2007 to 2008, attacks against DoD information systems went from 43,880 to 54,640, an increase of almost 20 percent. If trends from the first half of 2009 continue through the rest of the year, attacks will have reached approximately 87,570, a sixty percent increase from 2008.[4] This rise coincides with a large increase in attacks on other U.S. government agencies over the same period.[5]

Each of these penetrations involves a series of actions that do not differ substantially whether the intruder is acting on behalf of a terrorist group, a foreign government, a corporation, or is acting as an individual. The severe intrusions into cyber systems involve penetrating system security, navigating and mapping the cyber system, targeting the nodes that control the system and contain the most critical data, and often, extracting the data. At the same time, an intruder might leave behind a malicious software that could be activated later to regain entry or disrupt the affected system.[6]

General James E. Cartwright, then the commander of the U.S. Strategic Command (USSTRATCOM), told our commission in March 2007, that "China is actively engaged in cyber reconnaissance by probing computer networks of U.S. government agencies as well as private companies."[7] General Cartwright pointed out to commissioners that the data from these reconnaissance efforts helps identify weak points in networks and that large amounts of data are extracted from systems in minutes, accomplishing in a short time what traditional human intelligence might gather over a much longer period of time. Finally, General Cartwright pointed out that the psychological effects, chaos and disruption caused by a major cyber attack could be at the magnitude of similar effects caused by a weapon of mass destruction. This last point is true regardless of what country, group, or person perpetrates an attack of that magnitude.

---

[4] See "China's Cyber Activities that Target the United States, and the Resulting Impacts on U.S. National Security," (Chapter 2, Section 4) in the U.S.-China Economic and Security Review Commission's forthcoming *2009 Annual Report to Congress*. The Report will be available in late November at http://www.uscc.gov.

[5] Despite my overall view on the Department of Homeland Security (see below), US-CERT seems to be making improvements. "Quarterly Trends and Analysis Report," *US-CERT*, June 16, 2009. (Vol. 4, iss. 1.) http://www.us-cert.gov/press_room/trendsanalysisQ109.pdf.

[6] The report published by the U.S. China Economic and Security Review Commission contains a case study that explains this in greater detail.

[7] An electronic copy of the hearing record is posted at the Commission's web site: http://www/uscc.gov/hearings/hearingarchive.php#hearings2007.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00175 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.138

As alarming as these figures are, anecdotal evidence conveys the actual impact of such attacks on American targets. Time Magazine reported in 2005 about the network penetration of Sandia National Nuclear Weapons Laboratory, which may have led to the loss of information on nuclear weapons systems and other advanced technologies with weapons applications.[8] Based on the volume of reporting, attacks like this seem to be more prevalent. The *Wall Street Journal* reported in April of this year about the compromise of defense contractor computer systems that contained sensitive data about an advanced U.S. fighter plane, the F-35 "Lightning II."[9] The same month, the paper published an article about the pervasive compromise of U.S. critical infrastructure nodes. Of course, I do not have to tell this Subcommittee about attacks over the past several years on the computers of Members of Congress such as Representatives Frank Wolf and Mark Kirk, or Senator Bill Nelson.[10] All of the aforementioned examples have been attributed, with various degrees of certainty, to China.

China has not confined its efforts to just cyber espionage. As I stated in a recent Op-Ed in the *Wall Street Journal*, China's military has long sought powerful offensive cyber warfare capabilities.

> *The PLA has been developing these [offensive cyber] capabilities since at least 2003, when the then-director of the PLA's electronic warfare department, Dai Qingmin, proposed a comprehensive information warfare effort, including cyber attack, electronic attack and coordinated kinetic attacks in military operations.*[11]

China's military planners envision the coordinated use of this strategy—what they call "Integrated Network Electronic Warfare" (INEW)—against an adversary to gain an advantage in the early stages of a military conflict.[12] This sort of multi-spectrum assault has potential implications that go well beyond the battlefield. Given the complex architecture of modern military command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems, there is little chance that cyber warfare would remain localized to a particular theater of conflict. Cyber attacks specifically targeting domestic civilian infrastructure cannot be ruled out, and indeed

---

[8] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *Time Magazine*, August 29, 2005. http://www.time.com/time/magazine/article/0,9171,1098961,00.html#ixzz0VuzohGK6.

[9] Siobhan Gorman, August Cole and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009. http://online.wsj.com/article/SB124027491029837401.html.

[10] For more information about these incidents, see "China's Cyber Activities that Target the United States, and the Resulting Impacts on U.S. National Security," (Chapter 2, Section 4) in the U.S.-China Economic and Security Review Commission's forthcoming *2009 Annual Report to Congress*. The Report will be available in late November at http://www.uscc.gov.

[11] Larry Wortzel, "China's Cyber Offensive," *Wall Street Journal*, November 1, 2009. http://online.wsj.com/article/SB10001424052748703399204574508413849779406.html.

[12] A more detailed description is available in "China's Cyber Activities that Target the United States, and the Resulting Impacts on U.S. National Security," (Chapter 2, Section 4) in the U.S.-China Economic and Security Review Commission's forthcoming *2009 Annual Report to Congress*. The Report will be available in late November at http://www.uscc.gov.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00176 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.139

some Chinese military theorists advocate such an approach in warfare.[13] China, therefore, bears close examination as we consider our own policies for defense.

Other countries and groups likely contemplate similar types of operations. After all, many of these concepts were based on what the United States and coalition partners did in military operations in Kosovo and both offensives in Iraq. Think about the havoc that would result if a terrorist attack of the magnitude of the one on New York and the Pentagon on September 11, 2001 were coordinated with a concerted cyber attack on U.S. civil infrastructure or our banking system. According to *The Wall Street Journal* we have already experienced intrusions into our electric grids that illustrate how vulnerable the nation remains, and malicious code may have been left behind.[14]

Executive Branch Roles and Missions

The United States must actively address the challenges to our cyber security. To help stem the penetrations of U.S. companies, the Federal Bureau of Investigation has developed a defensive security education program to help private industry respond to the threat. So has the Department of Homeland Security. Executive Order 12829 established the National Industrial Security Program (NISP) to protect some 12,000 contractors that handle classified government information in the performance of their contracts. The Defense Security Service administers this program, for the Department of Defense and 23 other federal agencies. The Defense Security Service points out that "US. Industry develops and produces much of our nation's defense technology-much of which is classified."[15]

The public-private partnership US-CERT (United States Computer Security Emergency Readiness Team) is charged with "providing response support and defense against cyber attacks for the Federal Civil Executive Branch (that is, all .gov domains) and information sharing and collaboration with state and local government, industry and international partners."[16] US-CERT is the operational arm of the National Cyber Security Division at the Department of Homeland Security. On October 30, 2009, Secretary Napolitano opened a National Cyber Security and Communications Integration Center, designed to "facilitate a coordinated system to detect threats and communicate protective measures to ...federal, state, local and private sector partners and the public."[17]

Still, we have to remediate some structural problems in the government's approach to securing our networks. In particular, I would like to address what appears to be an

---

[13] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in *Beyond the Strait: PLA Missions Other than Taiwan*, eds. Roy Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: Army War College Strategic Studies Institute, 2009), p. 258. *http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=910*.

[14] Siobhan Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009. *http://online.wsj.com/article/SB123914805204099085.html*.

[15] See *https://www.dss.mil/GW/ShowBinary/DSS/isp/industrial_sec.html*.

[16] See *http://www.us-cert.gov/aboutus.html*.

[17] http://www.dhs.gov/ynews/releaases/pr_1256914923094.shtm

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00177 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.140

ongoing debate about the respective roles of the soon to be operational United States Cyber Command (USCYBERCOM) and the Department of Homeland Security (DHS).

As a full disclosure, early in my career, I worked on National Security Agency (NSA) programs and continued to be associated with some of them throughout my military career. Therefore, I have to admit to some bias in favor of that agency. The NSA will likely be given the responsibility of also being the headquarters of the USCYBERCOM. My personal experience with NSA leads me to tell you that I have no reservations about that agency taking the lead in implementing U.S. cyber defenses. The NSA and its predecessor organizations have continuously—and successfully—handled technical operations for our government since World War I. The Agency has decades of institutional experience, and highly skilled personnel who can operate in the electronic and cyber realms. NSA personnel also have the crucial linguistic capabilities to support investigations of foreign intrusions. The NSA has international relationships with American friends and allies and a wide range of relationships across industry. It is therefore best qualified to head the government's efforts in the cyber realm. I also want to point out that as a counterintelligence special agent, a foreign intelligence collector and a signals intelligence collector I underwent days of training and continual re-instruction on the nuances of gathering critical intelligence while still protecting the privacy rights of American citizens. Our entire Intelligence Community gets such training.

While few dispute that the NSA should direct the United States' offensive cyber operations, some cite privacy concerns over NSA involvement in securing government networks. My experience is that the NSA is extremely sensitive to intelligence oversight issues; their operators get a great deal of training and have privacy concerns drilled into their heads by leaders, inspectors general, oversight personnel, and training officers. I am very comfortable with the job that NSA does to ensure that its employees adhere to laws limiting the collection of information on United States persons.

DHS should play a substantive role in the defense of our nation's cyber space and critical information systems. To be candid, however, that Department is new, has a broad range of responsibilities, is spread thin, and is still growing into its duties. My understanding is that DHS has run two national cyber exercises. But to my knowledge, there has not yet been a systematic examination of lessons learned from the exercises nor uniform application of standards for attempting to correct any problems revealed across government or in industry.[18]

DHS' agencies and personnel have difficult tasks before them and they are working hard to meet the challenges; but I would like to give them a little more time before saddling the Department with all of the government's cyber security responsibilities. DHS also has other challenges it has to meet to defend against terrorists and to secure the homeland. The Department is not yet inspecting a substantial portion of shipping containers or unaccompanied baggage. The US-Visit program may allow the Department to know who is entering the country and with what type of visa, but we still have no idea

[18] These exercises—Cyber Storm (February 2006) and Cyber Storm II (March 2008)—were a step in the right direction, but require follow-up.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00178 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.141

when or if the same people leave. I would prefer to have an agency with years of experience and success in electronic and cyber operations like the NSA take the lead.

If privacy for American citizens is a concern, also think about institutional culture. Since the time of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the 1975 Church Committee), agencies of the U.S. Intelligence Community have come under strict oversight and revised their training and operations. All of the agencies of the Intelligence Community must by law seek investigative warrants under the Foreign Intelligence and Surveillance Act to intrude into the privacy of Americans. If I remember correctly my own training as a human intelligence collector and counterintelligence special agent, some of the agencies that formed DHS could (and still can) conduct intrusive, warrantless searches at our borders or customs searches with little probable cause other than the judgment of the agent. Our laws permit such searches for good reason under certain circumstances, but I would argue that the institutional culture in some agencies of DHS is very different than that in other law enforcement and intelligence agencies.

The Public-Private Relationship

Aside from structural decisions we make in government and the responsibilities in the National Security Council and White House, we need to bring in players from outside the government. The nation's critical infrastructure is owned and/or operated by the private sector.[19] In an October 2009 article, former acting Cyber Security Coordinator Melissa Hathaway highlighted the important role that the private sector must play to ensure our nation's resiliency in face of continuous malicious cyber activity. "Our government," she said, "must take bold steps to operationalize a partnership with industry. We need greater information sharing between the government and private sector on what is being targeted, and how."

Hathaway continued:

> *Our government cannot develop a strategy independent of private sector insight and cooperation. Our nation will need the private sector and its services and capabilities to find...[prevalent attack methodologies], inform the government of them and develop the solutions to resolve them. Our government needs to cultivate a public-private partnership and action plan that identifies the requirements for the future architecture, hardware, software and services that enable security and resilience. I believe that the private sector is ready to work with government on these efforts, and in order to take advantage of this*

[19] I have given this topic more extensive treatment in Larry Wortzel, "Securing America's Critical Infrastructures: A Top Priority for the Department of Homeland Security," *The Heritage Foundation*. May 7, 2003. http://www.heritage.org/Research/HomelandSecurity/hl787.cfm. See also See Larry M. Wortzel and Michael Scardaville, "The New Agenda for Homeland Security," *Heritage Foundation Executive Memorandum #779*, September 28, 2001.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00179 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.142

opportunity, the government must actively engage the private sector and set aggressive milestones toward achieving common goals. [20]

I would add that the government has a key responsibility here: to facilitate information sharing. This is where DHS could—and should—enable communication between all levels of government and relevant private entities. Moreover, it is critical that comprehensive guidelines for security best practices be developed and made available to the owners and operators of critical infrastructure. Congress has levers—such as tax incentives—that it should use to promote the adoption of these practices. In the absence of significant progress, Congress and the Administration should be willing to take a more active role in overseeing better security procedures.

International Cooperation and Cyber Defense Strategy

Parallel to our efforts at home, the United States must reach out to other nations to work against cyber threats. Japan, the United Kingdom, Estonia, Germany, and Australia, for example, have all reported malicious cyber activities targeting government systems. A more formal mechanism to exchange data about attacks would be tremendously helpful for investigators and to develop defenses. Such a mechanism should be established as soon as possible. Ideally, it would be in place and tested before a major computer crisis that requires rapid information sharing. The same urgency applies—perhaps to an even greater extent—to domestic information sharing processes across government and industry. This speaks to a more fundamental change we must make in our approach to cyber security: we must be more proactive. We can and should do more to get ahead of this problem, but it will take participation from all of the relevant stakeholders, facilitated by strong and centralized coordination.

Legislative Considerations

The National Research Council recently explored a number of issues related to cyber attacks and domestic law enforcement, not the least of which is the body of legislation on cyber matters.[21] I asked our staff at the U.S.-China Economic and Security Review Commission to put together a short, although perhaps not exhaustive, compendium for me on laws relating to cyber crimes and cyber security. I have attached their work as an appendix to this testimony.

It seems to me that one useful contribution from a legislative standpoint would be for Congress to update and coordinate these laws to ensure that all of the activities in the electronic, telecommunications and cyber domains permitted by law, as well as privacy and security considerations, are fully integrated. Also, I am not certain that implementing

---

[20] Melissa Hathaway, "Government Must Keep Pace with Cybersecurity Threats," *Information Security*, October 2009. http://searchsecurity.techtarget.com/magazinePrintFriendly/0,296905,sid14_gci1370150,00.html.

[21] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: The National Academies Press, 2009. See especially chapter 5, "Perspectives on Cyberattack Outside National Security," and Chapter 7, "Legal and Ethical Perspectives in Cyberattack."

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00180 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.143

regulations and Executive Orders are in place to ensure effective compliance with all the legislation. This is an area where the Congressional Research Service may be able to conduct a deeper study on the efficacy of integrating the legislation or the effectiveness of Executive Branch implementation. Alternatively, an audit by the Government Accountability Office may point the way for improvements in legislation, regulation, or oversight.

Chairman Cardin, Ranking Member Kyl, members of the Committee, thank you for your time and the opportunity to think more deeply about terrorism, protecting the privacy of Americans, and cyber security.

Larry M. Wortzel is vice chairman of the U.S.-China Economic and Security Review Commission. He is a retired Army colonel who served two tours of duty as a military attaché in China. Dr. Wortzel earned a Ph.D. in political science from the University of Hawaii – Manoa. He is a graduate of the U.S. Army War College and later served as director of the Strategic Studies Institute of that institution. For 25 years of his 32-year military career, Dr. Wortzel was an intelligence officer. He had assignments in human-source intelligence collection, signals intelligence collection, and foreign counterintelligence. After retiring from the Army, he was Asian studies director and vice president for foreign policy and defense studies at The Heritage Foundation.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00181 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.144

Appendix: Some of the Legislation Covering Cyber Crime, Cyber Security and Privacy in Electronic Communication[22]

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (18 U.S.C. § 1030) was passed by Congress in 1984 and subsequently amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, in 2002 by the Cyber Security Enhancement Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. The purpose of the CFAA is to reduce cracking of "protected computers" defined as "a computer used by the federal government or a financial institution, or one which is used in interstate or foreign commerce.

CFAA outlines seven types of criminal activity. They are listed below and have been revised according to the amendments made in 1986, 1994, 1996, 2001, and 2008:

1) Obtaining national security information from a computer without authorization and willfully communicating or transmitting the information

2) Compromising the confidentiality of a protected computer

3) Trespassing in a government computer

    - This includes those individuals who have no authorization to access a "nonpublic" computer. "Nonpublic" includes most government computers, but not Internet servers that, by design, offer services to members of the general public. For example, a government agency's database server is probably nonpublic, while the same agency's web servers and domain name servers are "public."

4) Accessing a computer to defraud and obtain value

    - This value must be greater than $5000 in a one year period.

5) Damaging a computer or information

    - This includes both causing damage intentionally and/or recklessly.

    - Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information." It includes economic loss (which can include time spent investigating and responding to attacks), threats to medical care, physical injury, threats to public health or security, and special harm to justice, national defense, or national security.

6) Trafficking in passwords

[22] All information from: *United States Department of Justice* "Prosecuting Computer Crimes Manual" February 2007. *http://www.justice.gov/criminal/cybercrime/ccmanual/index.html.*

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00182 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.145

- This transferring of passwords must affect interstate or foreign commerce, or computers used by and for the United States.

7) Extortion involving threats to damage computers, steal data on the computer, publicly display data, or not pay for damage already caused

   - This section applies, for example, to situations in which intruders threaten to penetrate a system and encrypt or delete a database. Other scenarios might involve the threat of distributed denial of service attacks that would shut down the victim's computers.

Wiretap Act and Electronic Communications Privacy Act

The Wiretap Act (18 U.S.C. § 2511) has as its dual purposes: "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." Although the original act covered only wire and oral communications, Congress amended it in 1986 to include electronic communications under the Electronic Communications Privacy Act. The 1986 amendment made the Wiretap Act another option for prosecuting computer intrusions that include real-time capture of information.

- The core prohibition of the Wiretap Act prohibits any person from intentionally intercepting, or attempting to intercept, any wire, oral, or electronic communication. Additionally, the Wiretap Act prohibits the "disclosure" or "use" of an intercepted message.

- Congress introduced amendments to this act in 1986 which stipulate that, in order to constitute a criminal violation, the interception of a covered communication must be "intentional"—deliberate and purposeful.

- The Wiretap Act defines an "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device."

- The Electronic Communications Privacy Act of 1986 (ECPA) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. The ECPA also added new provisions prohibiting access to stored electronic communications and included so-called pen/trap provisions that permit the tracing of telephone communications.

Other Statutes

- *Unlawful Access to Stored Communications* (18 U.S.C. § 2701) – focuses on protecting email and voicemail from unauthorized access.

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00183 Fmt 6633 Sfmt 6633 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.146

- *Identity Theft* (18 U.S.C. § 1028(a)(7)) and *Aggravated Identity Theft* (18 U.S.C. § 1028A) –applies to when network intrusions compromise the privacy of an individual because the data resides on the victim's network.

- *Access Device Fraud* (18 U.S.C. § 1029) - The term "access device" includes passwords, electronic banking account numbers, and credit card numbers. It can also be any card, serial number, or personal identification number.

- *CAN-SPAM Act* (18 U.S.C. § 1037) – provides a means for prosecuting those responsible for sending large amounts of unsolicited commercial email (a.k.a. "spam").

- *Wire Fraud* (18 U.S.C. § 1343) – pertains to fraud committed by means of fax, telex, modem, and Internet transmissions.

- *Communication Interference* (18 U.S.C. § 1362) – provides a means for prosecuting anyone who injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense fun

VerDate Nov 24 2008 09:56 Oct 29, 2010 Jkt 061662 PO 00000 Frm 00184 Fmt 6633 Sfmt 6011 S:\GPO\HEARINGS\61662.TXT SJUD1 PsN: CMORC

61662.147