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.

<u>Response to Question 1, all subparts:</u>

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 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.

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.

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.

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 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.***

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

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.

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

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.

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 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.

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 ~~in~~ability 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.

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.

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.

cdt
CENTER FOR DEMOCRACY & TECHNOLOGY

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

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

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.

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 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

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.

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.

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.

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.

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."

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 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.

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.

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.