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.