Department of Justice

STATEMENT OF

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

BEFORE THE

SENATE JUDICIARY COMMITTEE

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

AT A HEARING ENTITLED

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

PRESENTED

NOVEMBER 17, 2009

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

The Cyber Threat and the FBI's Cyber Program

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

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

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

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

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

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

FBI Leadership, Collaboration, and Information Sharing

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

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

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

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

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

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

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

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

FBI Investigative, Collaborative, and Information Sharing Success

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

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

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

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

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

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

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

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

The Way Ahead

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

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

Conclusion

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