Department of Justice

STATEMENT OF

JOSEPH M. DEMAREST, JR.
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE

ENTITLED

“CYBERSECURITY: ENHANCING COORDINATION TO PROTECT THE FINANCIAL SECTOR”

PRESENTED

DECEMBER 10, 2014

CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

Statement before the Senate Committee on Banking, Housing and Urban Affairs

Assistant Director Joseph M. Demarest, Jr.
Cyber Division, Federal Bureau of Investigation
December 10, 2014

Good morning Chairman Johnson, Ranking Member Crapo, and the distinguished members of this Committee. I am honored to appear before you today to discuss the cyber threats facing our nation, their relation to the financial sector, and the efforts the FBI is taking to identify, pursue, and defeat those threats.

In the course of my brief testimony, I hope to give you a sense of the extent to which today's cyber actors pose new and increasingly complex threats to our country and to the financial sector — a threat that challenges the traditional models of the law enforcement and intelligence communities, where threat actors were previously confined by time, distance, and physical location. Instead, today's cyber actors, from nation states to criminal groups and individuals, find themselves virtually unrestricted in their targets sets and their ambitions, launching attacks from all over the world at literally the speed of light. Today, I hope to convey the many ways that we at the FBI are doing everything in our power to protect the nation, and the financial sector in particular, from these threats.

Cyber Threats Against the Financial Sector: Trends and Implications

Before describing the current cyber threatscape, I'd like to give a brief overview of the FBI Cyber Division, our mission, and how we target the cyber adversaries that threaten this country on a daily basis. In general, the FBI's mission falls into three separate buckets: first, we *identify* the cyber actors perpetrating harm. In the world of cyber crime and cyber espionage, this is often the most difficult step, as cyber threats may hide in plain sight, using various methods to obfuscate their presence, location, and activities. Second, we *pursue* these actors, tracking their activity both online and off. To this end, we utilize collaborative partnerships across the federal government, with international partners and with industry, along with our unique combination of national security and law enforcement authorities, to gather intelligence about the tactics, techniques and procedures of these actors. In short, we find these threat actors and we watch them, gathering intelligence and understanding the motives and the conduct of our adversaries. Lastly, with the aid of partnerships and our unique authorities, we *defeat* cyber adversaries through a full range of methods, including – most importantly, arresting and prosecuting those responsible. The FBI focuses foremost on intelligence led, threat-focused cyber operations which our personnel, analysts, computer scientists, and agents in the field help us achieve every day.

As the members of this Committee are aware, the range of actors who threaten our interests is as complex as it is varied. We face cyber terrorists, who aim to use our reliance upon and use of digital systems to advance their political or ideological goals. We face nation states, who aim to use the cyber world to conduct espionage, to make preparations for war, and who may even carry out acts of war through cyber means. We face ideology-driven criminals, who may use methods such as denial of service attacks, known as "DDoS" attacks, to further their own ideology or social cause. We face insider threats, whose legitimate access to sensitive information may be used for various illicit ends. Lastly, we face financially motivated groups and individuals, who use a range of methods to enrich themselves at others' expense — and it is this group that I will focus upon most specifically today, though each and every group I just listed may, at times, view the financial sector as a prime target.

As the members of the Committee are also aware, the threat from cyber actors — specifically cyber criminals — continues to garner an increasing share of the media spotlight and continues to advance in sophistication. Recent high-profile attacks, such as those on eBay, Sony, J.P. Morgan Chase, and others, highlight vulnerabilities in some of our nation's largest companies. Regarding the threats to the financial sector in particular, such threats range in complexity, and we continue to work closely with the Secret Service, DHS, and other partners across the government. Point of sale thefts, also known as "POS" scams, for example, are not new, but continue to pose serious threats to the financial services industry. According to Verizon's 2014 Data Breach Investigations Report, the physical installation of a "skimmer" on an ATM, gas pump, or POS terminal to read credit card data has targeted ATMs with an overwhelming specificity — 87 percent of skimming attacks in 2013, for example, were on ATMs. Retail POS scams, where attackers compromise the computers and servers that run POS applications with the intention of capturing payment data, comprise an additional level of sophistication, and can take weeks or even months to be discovered, little less mitigated. The high-profile attack on Target provides one of the more sophisticated examples of retail POS scams, in which, according to open source reporting, 40 million credit card numbers and another 70 million customer records were stolen. Such attacks are not unique to Target — additional data breaches have been reported at Neiman Marcus, Michaels, and P.F. Chang's, among many others.

Vulnerabilities in mobile banking pose another new and highly sophisticated danger, as mobile banking vulnerabilities may exist on mobile devices that are not patched, and malware can be developed to specifically target the use of mobile devices. One example of this type of vulnerability is the Zeus-in-the-Middle malware, a mobile version of the GameOver Zeus malware, which itself was one of the most sophisticated types of malware the FBI ever attempted to disrupt. GameOver Zeus was designed to steel banking credentials that criminals could then use to initiate or redirect wire transfers to overseas bank accounts. All told, the malware infected over 1 million computers worldwide and caused over $100 million in estimated losses. Zeus-in-the-Middle has not caused the same level of damage or losses as GameOver Zeus, but its very existence illustrates the risk posed to mobile platforms, where devices can be infected by malicious apps or via spear phishing emails, and which can then enable cyber criminals to utilize the banking credentials of targeted users on a grand scale. Current open source reporting suggests that Android OS devices remain a prime target for mobile malware — according to the 2014 Cisco Annual Security Report, for example, 99 percent of mobile malware in 2013 targeted the Android platform.

Botnets, which can harness the power of an enormous web of computers for malicious purposes, continue to evolve as well. As I speak, estimates place the total damages caused by botnets at more than $9 billion in losses to U.S. victims and over $110 billion in losses worldwide. Approximately

500 million computers are infected globally per year — translating to 18 victims per second. As botnets become more sophisticated, our techniques must evolve to keep pace. The FBI and our partners may take down one botnet, for example, but coders may alter code and rebuild their bots in fairly short order. The power and scale of botnets is particularly worth noting, as botnets have been used to attack the financial sector through DDoS attacks, and the FBI has been deeply involved in preventing such attacks and in keeping such attacks from inflicting lasting damage. Beginning in September 2012, for example, actors launched powerful DDoS attacks from a botnet, combining the bandwidth of numerous web servers to target major U.S. banking institutions. The FBI worked closely with Department of Homeland Security (DHS) to issue Joint Indicator Bulletins (JIBs) to the U.S. banks, which included thousands of IP addresses that participated in the attacks. The U.S. banks used the IP addresses to better mitigate future incidents, thus helping to ensure their business operations could proceed with less interruption of service to their customers. The JIBs helped reduce the resources available for the threat actors to carry out future DDoS operations and demonstrated the effectiveness of FBI outreach to industry. Throughout this campaign, the FBI held significant outreach efforts to brief bank net-defenders through a series of classified briefs. These briefs, conducted by FBI, DHS, and Treasury representatives, provided bank security personnel the context of the DDoS threat and enabled the banks to share best-practices with their peers in real-time.

From March 2013 to July 2014, the FBI provided approximately 36 classified threat briefings regarding the DDoS attacks to private sector financial institutions and governmental agencies, including DHS, Department of Treasury, the Federal Deposit Insurance Corporation, and the Federal Reserve System. The initial classified briefing, held on March 19, 2013, was attended by over 300 chief information security officers via secure video teleconference from 33 FBI field offices. This type of outreach is far from irregular — based on imminent threats to the financial sector in early 2014, the FBI provided classified threat briefings in March, April, and July 2014 to a total of 145 financial institutions.

We at the FBI, in short, are doing everything in our power to keep pace with the evolving threat against the financial sector. We further our law enforcement mission when we collaborate within the government and across the private sector to prosecute and protect our nation and industries from the devastating consequences of cyber attacks.

Coordination and Information Sharing Across the Government

The FBI and our partners throughout the government have all made significant progress in recent years in collaborating within the cyber domain — and our progress hasn't just been limited domestically, but has occurred at international levels as well. A decade ago, for example, if an FBI agent tracked an Internet Protocol (IP) address to a criminal investigation, and if that IP address was located in a foreign country, this meant the effective end of the investigation. Since that time, however, the FBI has placed cyber specialists in key international locations to facilitate the investigation of cyber crimes affecting the U.S. Recognizing the value of cyber specialists working with key international partners, the FBI Cyber Division stood up a team known as the Operational Coordination Unit's Extraterritorial Operations group to focus on supporting, coordinating, and providing oversight of international cyber national security and criminal intrusion investigations and operations. This group assesses the global cyber threat environment, developing and executing plans to ensure the assignment of FBI cyber specialists to areas where they are most needed. Such developments, along with technical improvements in our ability to track IP addresses back to their source, has led key actors in the underground economy to recognize the following fact: there are fewer and fewer safe hiding places around the globe for cyber criminals. These criminals may be able to run, capitalizing upon the anonymity and the geographical dispersion of the Internet, but thanks to our efforts, they will not be able to hide for long.

One prime example of the importance of collaboration and coordination is the recent takedown of Silk Road 2.0. Beginning in late December 2013, Blake Benthall, also known by the online handle "Defcon," secretly owned and operated an underground website known as Silk Road 2.0 — one of the most extensive, sophisticated, and widely used criminal marketplaces ever created on the Internet. The website operated on the Tor network, a special network of computers distributed around the world and designed to conceal the IP addresses of the computers that access the network, thereby masking the identities of the network's users. Silk Road 2.0 launched in November 2013 after its predecessor was shut down by law enforcement. Since its launch in 2013, Silk Road 2.0 has been used by thousands of illicit actors to distribute hundreds of kilograms of illegal drugs and other illegitimate goods and services to buyers throughout the world, as well as to launder millions of dollars generated by these unlawful transactions. As of September 2014, Silk Road 2.0 was generating sales of at least approximately $8 million per month and had approximately 150,000 active users. The very existence of Silk Road 2.0 highlights the core concern I'm here to address today: cyber criminals now operate far outside the traditional bounds that confined criminals in past decades, selling banking credentials by the thousands and placing malware on the market for the purposes of DDoS attacks, to cite just two examples of illicit activities that target the financial sector. Whereas last century's bank robbers used an automobile to steal from a handful of banks in a few states in one day — a novel development for the time — today's bank robbers can use the Internet to steal money from thousands of banks across the world in a few hours, all without ever leaving their basement.

Thanks to our coordinated efforts, however, criminal marketplaces like Silk Road 2.0 cannot and will not last for long. The investigation into Silk Road 2.0 was conducted jointly by the FBI and the DHS's Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI), illustrating the critical nature of cooperation and information sharing in today's cyber investigations — no government agency, no matter how competent its agents and experts, can operate successfully on its own. We capitalize on our distinct roles and responsibilities within the government to address and prevent cybercrime. Over the course of the investigation into Silk Road 2.0, an HSI agent acting in an undercover capacity successfully infiltrated the support staff involved in the administration of the Silk Road 2.0 website and was given access to private, restricted areas of the site reserved for Benthall and his administrative staff. By doing so, the HSI agent was able to interact directly with Benthall throughout his operation of the website.

On November 7, 2014, the U.S. government seized the Silk Road 2.0 website in the largest law enforcement action to date against criminal websites operating on the Tor network. Benthall was arrested and charged with one count of conspiring to commit narcotics trafficking (carrying a maximum sentence of life in prison and a mandatory minimum sentence of 10 years in prison), one count of conspiring to commit computer hacking (carrying a maximum sentence of five years in prison), one count of conspiring to traffic in fraudulent identification documents (carrying a maximum sentence of 15 years in prison), and one count of money laundering conspiracy (carrying a maximum sentence of 20 years in prison). The investigation was a key success for the FBI, for ICE-HSI, and for the U.S. government as a whole — and a key illustration of the importance of collaboration and cooperation.

Another example of the importance of collaboration and cooperation, both inside and outside of government, is the vital work the National Cyber Investigative Joint Task Force (NCIJTF) performs on a daily basis. Mandated by the President in 2008, the NCIJTF serves as national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations among 19 federal agencies. The FBI aims to strengthen and solidify the NCIJTF as the cybersecurity center for coordinating cyber threat investigations and disruption operations. The NCIJTF involves senior personnel from key agencies, including deputy directors from the National Security Agency, the Department of Homeland Security, the Central Intelligence Agency, the U.S. Secret Service, and U.S. Cyber Command. Reinforcing the role of the NCIJTF on cross-government cyber threat information sharing and coordination is a key priority for the FBI.

Lastly, the FBI is working to strengthen local and national information sharing and collaboration efforts in support of network defense, intelligence operations, and disruption operations. And I cannot make the following statement frequently enough: the private sector is an essential partner if we are to succeed in defeating the cyber threat our nation confronts. I will discuss in more detail some of our collaboration efforts with the private sector shortly.

Current FBI Efforts to Combat Cyber Threats

The FBI is engaged in a host of efforts to combat cyber threats, from efforts focused on threat identification and sharing inside and outside of government, to our internal emphasis on developing and retaining new talent and changing the way we operate to evolve with the cyber threat. I would like to take this opportunity to highlight a few of the ways we at the FBI are confronting this threat head on.

FBI Liaison Alert System

As I alluded to earlier in my testimony, the threat of botnets provides a good example of how the FBI is proactively working with industry partners to combat cyber threats. To further assist with network defense and mitigation of botnets, the FBI created a document called the FBI Liaison Alert System message, or FLASH. Through the system, the FBI releases high confidence data to the private sector with indicators and alerts related to computer intrusions and DDoS attacks. From April 2013 to July 2014, the FBI disseminated 34 FLASH messages, about 20 of which dealt with threats against the financial sector. The FBI disseminated, among other information, indicators for approximately 115,000 compromised systems in these FLASH messages. These declassified, technical indicators, associated with intrusions, are meant to enable industry partners to be on the lookout for and defend their infrastructure from nefarious traffic on their networks.

The FBI provided these FLASH messages to key partners across affected critical infrastructure sectors, to include: Tier 1 and 2 Internet Service Providers (ISPs), Domain Name Server (DNS) root server operators, top-level domain (TLD) operators, and Five Eyes partners. When the FBI receives credible information regarding a threat to U.S. critical infrastructure, FBI coordinates with DHS to discuss and deconflict victim notification and mitigation strategies, at times involving other agencies, such as the Department of Treasury, as well.

Guardian Victim Analysis Unit

The FBI's Guardian Victim Analysis Unit (GVAU) is a direct response to the President's 2013 Executive Order 13636, which called for increases in the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better defend themselves against cyber threats. To help aid these entities and to enhance private sector information sharing efforts, the FBI established Cyber Guardian, a series of applications that enables actors in and outside of government to share threat information. One Cyber Guardian application is available on a Secret enclave, and two applications known as eGuardian and iGuardian/InfraGard — both operating at the unclassified level — are available to State, Local, Tribal, and Territorial (SLTT) entities, and to the private sector, respectively. The Cyber Guardian applications provide a means for the FBI to rapidly disseminate reports on cyber threat activity, in addition to a platform for coordination and deconfliction of cyber threat information.

The Internet Crime Complaint Center

Established in 2000, the Internet Crime Complaint Center (IC3) is a partnership between the FBI and the National White Collar Crime Center meant to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. During its infancy, the IC3 received approximately 2,000 victim complaints per month. Now the IC3 receives approximately 800 complaints a day, with over 244,000 complaints received to date for the 2014 calendar year. In 2013, the IC3 received 262,813 consumer complaints with losses in excess of $781 million. The IC3 database currently houses more than 3.15 million consumer complaints dating back to its inception in 2000.

The Domestic Security Alliance Council

The Domestic Security Alliance Council (DSAC) is a strategic partnership between the U.S. government and U.S. private industry, formed with the goal of increasing security by enhancing communications and promoting the timely and effective exchange of security information among its constituents. The DSAC advances the FBI's mission of preventing, detecting, and deterring criminal acts by facilitating strong, enduring relationships among its private industry members, FBI headquarters divisions, FBI field offices, DHS headquarters, DHS fusion centers, and other federal government entities.

The National Cyber-Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance (NCFTA) is composed of representatives of industry, academia, and the FBI, all working together to collaborate on combating cyber crime. The NCFTA provides a unique environment for information sharing between law enforcement, private industry, and academia. The NCFTA is a non-profit group whose members include ISPs, banks, retailers, and a whole host of other industry representatives, along with law enforcement and academia, with a mission to identify cyber threats and share information for mitigation and neutralization purposes. The NCFTA provides a one-of-a-kind opportunity for subject matter experts to address global cyber threats such as botnets, spam, and malware. Because of its non-profit status, the group can share information in a neutral environment, develop a strategic understanding of the threat, and work to address cyber threats collaboratively.

National Industry Partnership Unit

The FBI established an entity known as the National Industry Partnership Unit to develop partnerships through the InfraGard program between the FBI and private sector, academic, and other public entities, to support the FBI's investigative programs. Established in the Cleveland field office in 1996, InfraGard was initially a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. InfraGard soon expanded to other FBI field offices, and in 2003 the Cyber Division assumed responsibility for the program. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard members gain access to information that enables them to protect their assets and in turn give information to the government that facilitates its responsibilities in preventing and addressing terrorism and other crimes. This relationship supports information sharing at both the national and local levels, with the aim of increasing the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime, and other major crime programs.

Charting the Cyber Future

The future cyber threatscape will certainly be complex — based on recent advances in the sophistication of our adversaries, both state and non-state, it is hard to imagine what this threatscape will look like 10 or even 20 years down the road. Nevertheless, we in the FBI pride ourselves on being a forward looking organization, and adapting to the challenges we face. The FBI Cyber Division — our agents, computer scientists, analysts, and personnel — are all working hard to outpace such threats on a daily basis, identifying, pursuing, and defeating our adversaries, wherever in the world they might be.

There are, however, a number of ways that Congress might seek to aid us in our efforts. In particular, I would like to enumerate three concerns that new legislation or amendments to existing legislation could address that would strengthen our ability to combat cyber threats, as follows:

- <u>Updating the Computer Fraud and Abuse Act.</u> The Computer Fraud and Abuse Act (CFAA) constitutes the primary federal law against hacking, protecting the public against criminals who hack into computers to steal information, install malicious software, and delete files. The CFAA was first enacted in 1986, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement with the tools to respond to changing

> threats. The CFAA has not been amended since 2008, however, and the intervening years have again created the need for the enactment of modest, incremental changes. The Administration has proposed several such revisions to keep federal criminal law up-to-date with rapidly-evolving technologies.

Cyber threats adapt and evolve at the speed of light, and we need laws on the books that reflect the most current means by which cyber actors are committing crimes. Updating the CFAA to reflect these changes would help strengthen our ability to punish, and therefore to deter, the crimes we seek to prevent.

Data Breach Notifications. We believe there is a strong need for a uniform federal standard holding certain types of businesses accountable for data breaches and theft of electronic personally identifiable information. Businesses should, for example, be required to provide prompt notice to consumers in the wake of a certain cyber attacks. Such a standard would not only hold businesses accountable for breaches, but would also assist in FBI and other law enforcement efforts to identify, pursue, and defeat the perpetrators of cyber attacks.

Information Sharing. Although the government and the private sector already share cyber threat information on a daily basis, legislation can enhance the value and benefit of these information sharing relationships. The government and the private sector both have critical and unique insights into the cyber threats we face, and sharing these insights is necessary to enhance our mutual understanding of the threat. Similarly, the operational collaboration required to identify cyber threat indicators and to mitigate intrusions requires the exact type of sharing we seek in the first place. As such, the FBI supports legislation that would establish a clear framework for sharing and reduce risk in the process, in addition to providing strong and straightforward safeguards for the privacy and civil liberties of Americans. U.S. citizens must have confidence that threat information is being shared appropriately, and we in the law enforcement and intelligence communities must be as transparent as possible. We also want to ensure that all the relevant federal partners receive the information in real time.

The bottom line, however, is that current levels of information sharing are insufficient to address the cyber threats we face, specifically with regards to the financial sector. The U.S. is currently facing sophisticated, well-resourced adversaries, and minimum security requirements are needed to harden our critical infrastructure networks. The government and private sector should collaborate to develop these requirements, and we believe that legislation would help to further these ends. There are a host of statutory and regulatory restrictions as well that provide narrowly tailored liability protections for appropriate cyber information sharing. Further, there are a number of regulatory and statutory concerns that private actors may express when it comes to sharing cyber threat information with the government, and new legislation can and should be crafted to address these concerns. The events of the last year, and the continuing high-profile cyber attacks on major American companies, should serve to highlight the need for new engagement against cyber threats on every level possible.

In the absence of the passage of cybersecurity legislation, however, the administration is taking steps in the right direction to ensure that we can share information, in a practical and meaningful way. One such step is Executive Order (EO) 13636, entitled “Improving Critical Infrastructure Cybersecurity” and which I addressed briefly earlier, signed by the President in February 2013 and designed to provide critical infrastructure owners and operators with assistance to address cyber threats and manage risks. The EO calls for the government to collaborate more closely with industry by sharing information about cyber threats and jointly developing a framework of cybersecurity standards and best practices. One of the EO’s main goals is to improve government information sharing with critical infrastructure owners and operators regarding cyber threats, including attack signatures and other technical data. The FBI would, however, welcome more active engagement from Congress on these matters. Although the EO is a step in the right direction, robust cybersecurity legislation is still needed. As partners across the government and private sector have explored the ways we can operate, under existing laws, to implement the requirements of the EO, we are well positioned to have a more informed dialogue with Congress, and to improve our ability to address cyber threats.

Conclusion

In conclusion, Mr. Chairman, the FBI is focusing our resources, expanding our presence at the local, national and international levels, and engaging in cooperation with the private sector and intergovernmental collaboration. As the Committee knows well, we face considerable challenges in our efforts to combat cyber crime, and yet we remain optimistic that by identifying, pursuing, arresting and prosecuting these offenders we will defeat our cyber adversaries and continue to succeed in neutralizing these threats. My colleagues at the FBI and I look forward to working with the Committee and with Congress in protecting our nation from the evolving threat posed by cyber actors. Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.