Department of Justice

STATEMENT OF

ROBERT ANDERSON, JR.
EXECUTIVE ASSISTANT DIRECTOR
CRIMINAL, CYBER, RESPONSE, AND SERVICES BRANCH
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ENTITLED

"CYBERSECURITY, TERRORISM, AND BEYOND:
ADDRESSING EVOLVING THREATS TO THE HOMELAND"

PRESENTED

SEPTEMBER 10, 2014

Statement of
Robert Anderson, Jr.
Executive Assistant Director
Criminal, Cyber, Response, and Services Branch
Federal Bureau of Investigation
Department of Justice

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

Entitled
"Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland"

Presented on
September 10, 2014

Good morning Chairman Carper and Ranking Member Coburn. I appreciate the opportunity to appear before you today to discuss cyber, terrorism, and other threats to our nation and how the FBI is collaborating with our partners in government, law enforcement, and the private sector to prevent and combat them.

The Cyber Threat and FBI Response

We face cyber threats from state-sponsored hackers, hackers for hire, global cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us. They seek to strike our critical infrastructure and to harm our economy.

Given the scope of the cyber threat, agencies across the Federal government are making cyber security a top priority. We and our partners at the Department of Homeland Security (DHS), the National Security Agency, and other U.S. Intelligence Community and law enforcement agencies have truly undertaken a whole-of-government effort to combat the cyber threat. Within the FBI, we are prioritizing high-level intrusions—the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We are working with our counterparts to predict and prevent attacks, rather than simply react after the fact.

FBI agents, analysts, and computer scientists use technical capabilities and traditional investigative techniques—such as sources and wiretaps, surveillance, and forensics—to fight cyber crime. We work side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and at the National Cyber Investigative Joint Task Force (NCIJTF). Through our 24-hour cyber command center, CyWatch, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to Federal cyber centers, government

agencies, FBI field offices and legal attachés, and the private sector in the event of a significant cyber intrusion.

We also exchange information about cyber threats with the private sector through partnerships such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance (NCFTA).

For our partners in State and local law enforcement, we have launched Cyber Shield Alliance on www.leo.gov, which provides access to cyber training opportunities and information, as well as the ability to report cyber incidents to the FBI.

In addition, our legal attaché offices overseas work to coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. We are supporting and collaborating with newly established cyber crime centers at Interpol and Europol. We continue to assess other locations to ensure that our cyber personnel are in the most appropriate locations across the globe

We know that to be successful in the fight against cyber crime, we must continue to recruit, develop, and retain a highly skilled workforce. To that end, we have developed a number of innovative staffing programs and collaborative private industry partnerships to ensure that over the long term we remain focused on our most vital resource—our people.

As the committee is well aware, the frequency and impact of cyber attacks on our nation's private sector and government networks have increased dramatically in the past decade, and are expected to continue to grow. Since 2002, the FBI has seen an 80 percent increase in the number of computer intrusion investigations.

Recent Successes

Over the past several months, the FBI and the Justice Department have announced a series of separate indictments of overseas cyber criminals.

In an unprecedented indictment in May, we charged five Chinese hackers with illegally penetrating the networks of six U.S. companies. The five members of China's People's Liberation Army allegedly used their illegal access to exfiltrate proprietary information, including trade secrets.

Later that month, we announced the indictments of a Swedish national and a U.S. citizen believed to be the co-developers of a particularly insidious computer malware known as Blackshades. This software was sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide.

In June, the FBI announced a multinational effort to disrupt the GameOver Zeus botnet, the most sophisticated botnet that the FBI and its allies had ever attempted to disrupt. GameOver Zeus is believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world. This effort to disrupt it involved notable cooperation with the

private sector and international law enforcement. GameOver Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to GameOver Zeus are estimated to be more than $100 million.

Just last month, a Federal grand jury indicted Su Bin, a Chinese national, on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft. Su is currently in custody in British Columbia, Canada, where he is being held pursuant to a provisional arrest warrant submitted by the United States. The charges carry a total maximum statutory penalty of 30 years in prison. The investigation in this case was conducted by the Federal Bureau of Investigation and the Air Force Office of Special Investigations.

The Blackshades and GameOver Zeus indictments are part of an initiative launched by the FBI Cyber Division in April 2013 to disrupt and dismantle the most significant botnets threatening the economy and national security of the United States. This initiative, named Operation Clean Slate, is the FBI's broad campaign to implement appropriate threat neutralization actions through collaboration with the private sector, DHS, and other United States government partners, as well as our foreign partners. This includes law enforcement action against those responsible for the creation and use of the illegal botnets, mitigation of the botnet itself, assistance to victims, public service announcements, and long-term efforts to improve awareness of the botnet threat through community outreach. Although each botnet is unique, Operation Clean Slate's strategic approach to this significant threat ensures a comprehensive neutralization strategy, incorporating a unified public/private response and a whole-of-government approach to protect U.S. interests.

The impact of botnets has been significant. Botnets have been estimated to cause more than $113 billion in losses globally, with approximately 375 million computers infected each year, equaling more than one million victims per day, translating to 12 victims per second.

Another Operation Clean Slate success came in January 2014, when Aleksandry Andreevich Panin, a Russian national, pled guilty to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the malicious software known as Spyeye, which infected more than 1.4 million computers in the United States and abroad. Based on information received from the financial services industry, more than 10,000 bank accounts had been compromised by Spyeye infections in 2013 alone. Panin's co-conspirator, Hamza Bendelladj, an Algerian national who helped Panin develop and distribute the malware, was also arrested in January 2013 in Bangkok, Thailand.

In addition to these recent investigative successes against cyber threats, we are continuing to work with our partners to prevent attacks before they occur.

One area in which we have had great success with our overseas partners is in identifying and targeting infrastructure we believe has been used in distributed denial of service (DDoS) attacks,

and preventing that infrastructure from being used for future attacks. A DDoS attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network.

Since October 2012, the FBI and DHS have released more than 170,000 Internet Protocol addresses of computers that were believed to be infected with DDoS malware. We have released this information through Joint Indicator Bulletins (JIBs) to more than 130 countries via DHS's National Cybersecurity and Communications Integration Center (NCCIC), where our liaisons provide expert and technical advice for increased coordination and collaboration, as well as to our legal attachés overseas.

These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDoS attacks. We are continuing to target botnets through this strategy and others.

In 2013, for example, the FBI created FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs) to release industry-specific details on current and emerging threat trends, and technical indicators to the private sector. To date, the FBI has disseminated 40 FLASH messages, 21 of which dealt with threats to the financial industry. These PIN and FLASH messages were created to proactively deliver timely, actionable intelligence to potential victims and law enforcement partners at the international, State, and local levels.

Next Generation Cyber Initiative

The need to prevent attacks is a key reason the FBI has redoubled our efforts to strengthen our cyber capabilities while protecting privacy, confidentiality, and civil liberties. The FBI's Next Generation Cyber Initiative, which we launched in 2012, entails a wide range of measures, including focusing the Cyber Division on intrusions into computers and networks—as opposed to crimes committed with a computer as a modality hiring additional computer scientists to assist with technical investigations in the field; and expanding partnerships and collaboration at the NCIJTF. In addition, after more than a decade of combating cybercrime through a nationwide network of interagency task forces, the FBI has evolved its Cyber Task Forces in all 56 field offices to focus exclusively on cybersecurity threats.

At the NCIJTF—which serves as a coordination, integration, and information sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations—we are coordinating at an unprecedented level. This coordination involves senior personnel at key agencies. NCIJTF, which is led by the FBI, now has deputy directors from the NSA, DHS, the Central Intelligence Agency, U.S. Secret Service, and U.S. Cyber Command. In the past year, three of our Five Eyes international partners joined us at the NCIJTF: Australia embedded a liaison officer in May 2013, the UK in July 2013, and Canada in January 2014. By developing partnerships with these and other nations, NCIJTF is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries.

Private Sector Outreach

In addition to strengthening our partnerships in government and law enforcement, we recognize that to effectively combat the cyber threat, we must significantly enhance our collaboration with the private sector. Our nation's companies are the primary victims of cyber intrusions, and their networks contain the evidence of countless attacks. In the past, industry has provided us information about attacks that have occurred, and we have investigated the attacks—but we have not always provided information back.

To remedy that, the Cyber Division has established a Key Partnership Engagement Unit (KPEU) to manage a targeted outreach program focused on building relationships with key private sector corporations. The unit works to share sector-specific threat information with our corporate partners.

We have provided a series of classified briefings for key sectors, including financial services and energy, to help them repel intruders.

Through the FBI's InfraGard program, the FBI develops partnerships and working relationships with private sector, academic, and other public-private entity subject matter experts. Primarily geared toward the protection of critical national infrastructure, InfraGard promotes ongoing dialogue and timely communication among a current active membership base of more than 25,000.

InfraGard members are encouraged to share information with government that better allows government to prevent and address criminal and national security issues. Active members are able to report cyber intrusion incidents in real-time to the FBI through iGuardian, which is based on our successful counterterrorism reporting system known as Guardian.

Just last month, the FBI deployed a malware repository and analysis system called Malware Investigator to our domestic and foreign law enforcement partners and members of the U.S. Intelligence Community. The system allows users to submit malware directly to the FBI and quickly receive technical information about the samples to its users so they can understand how the malware works. It also enables the FBI to obtain a global view of the malware threat. Beyond technical reporting, Malware Investigator identifies correlations that will allow users to "connect the dots" by highlighting instances in which malware was deployed in seemingly unrelated incidents.

The FBI's Cyber Initiative and Resource Fusion Unit (CIRFU) maximizes and develops intelligence and analytical resources received from law enforcement, academia, international, and critical corporate private sector subject matter experts to identify and combat significant actors involved in current and emerging cyber-related criminal and national security threats. CIRFU's core capabilities include a partnership with the National Cyber Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania, where the unit is collocated with CIRFU. NCFTA acts as a neutral platform through which the unit develops and maintains liaison with hundreds of formal and informal working partners who share real-time threat information and

best practices and collaborate on initiatives to target and mitigate cyber threats domestically and abroad.

The FBI recognizes that industry collaboration and coordination are critical in our combating the cyber threat effectively. As part of our enhanced private sector outreach, we have begun to provide cleared industry partners with classified threat briefings and other information and tools to better help them repel intruders.

Counterterrorism and Other Threats

Though the cyber threat is one of the FBI's top priorities, combating terrorism remains our top investigative priority. As geopolitical conflict zones continue to emerge throughout many parts of the world, terrorist groups may use this instability to recruit and incite acts of violence.

The continuing violence in both Syria and Iraq and the influx of foreign fighters threatens to destabilize an already volatile region while also heightening the threat to the West. Due to the prolonged nature and the high visibility of the Syrian conflict, we are concerned that U.S. persons with an interest in committing jihad will be drawn to the region. We can address this issue more fully in the closed session.

***

In conclusion, Chairman Carper, to counter the threats we face, we are engaging in an unprecedented level of collaboration within the U.S. government, with the private sector, and with international law enforcement.

We are grateful for the committee's support and look forward to continuing to work with you and expand our partnerships to defeat our adversaries.