Department of Justice

STATEMENT OF

RICHARD A. MCFEELY
EXECUTIVE ASSISTANT DIRECTOR
CRIMINAL, CYBER, RESPONSE AND SERVICES BRANCH
FEDERAL BUREAU OF INVESTIGATION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON APPROPRIATIONS
UNITED STATES SENATE

ENTITLED

# “CYBERSECURITY: PREPARING FOR AND RESPONDING TO THE ENDURING THREAT”

PRESENTED

JUNE 12, 2013

Statement of Richard A. Mcfeely
Executive Assistant Director
Criminal, Cyber, Response and Services Branch
Federal Bureau of Investigation
U.S. Department of Justice

Before the Committee on Appropriations
United States Senate

"Cybersecurity: Preparing for and Responding to the Enduring Threat"
June 12, 2013

Good afternoon Chairwoman Mikulski, Vice Chairman Shelby, and members of the Committee. I appreciate the opportunity to appear before you today to discuss the cyber threat, how the FBI has responded to it, and how we are marshaling our resources and strengthening our partnerships to more effectively combat the increasingly sophisticated adversaries we face in cyberspace.

## *The Cyber Threat*

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 84 percent increase in the number of computer intrusion investigations.

Our adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement. It is difficult to overstate the potential impact these threats pose to our economy, our national security, and the critical infrastructure upon which our country relies. The bottom line is we are losing data, money, ideas, and innovation to a wide range of cyber adversaries and much more is at stake.

Director Mueller has said he expects the cyber threat to surpass the terrorism threat to our nation in the years to come. That is why we are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11th attacks.

## *FBI Response*

The FBI recognized the significance of the cyber threat more than a decade ago and, in response, created the Cyber Division and elevated the cyber threat to our number three national priority (only after counterterrorism and counterintelligence). We also significantly increased our hiring of technically trained agents, analysts, and forensic specialists and expanded our partnerships with law enforcement, private industry, and academia.

We have made great progress since the Cyber Division was first created in 2002. Prior to that, we considered it a success when we recognized that networks were being attacked. We soon enhanced our ability to determine attribution—knowing *who* was breaking into our computers and networks—and to track Internet Protocol (IP) addresses back to their source. Now, the question we ask ourselves is, "How are we going to take action on that information?"

The perpetrators of these attacks are often overseas, but in the past, tracking an IP address back to its source in a foreign country usually led to a dead end. To address this problem, we embedded cyber agents with law enforcement in several key countries, including Estonia, Ukraine, the Netherlands, Romania, and Latvia. We have also worked with several of these countries to extradite subjects from their countries to stand trial in the United States.

Building on the success of our international outreach, we are currently expanding our Cyber Assistant Legal Attaché program to the United Kingdom (U.K.), Singapore, Bulgaria, Australia, Canada, the Republic of Korea, and Germany.

***Recent Successes***

A prime example of international collaboration came in the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme. The scheme infected more than four million computers in more than 100 countries with malware. The malware secretly altered the settings on infected computers, enabling the hackers to hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-route computers to certain Web sites and ads. The company received fees each time these web sites or ads were clicked on or viewed by users and generated $14 million in illegitimate income for the operators of Rove Digital.

Following the arrest of several alleged co-conspirators in Estonia, FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data linking them to the scheme. Seven individuals have been indicted in the Southern District of New York in this case. Two of the six for which the United States sought extradition have been remanded to U.S. custody and have recently pleaded guilty to wire fraud and computer intrusion.

While the FBI and our partners have had multiple recent investigative successes against the threat, we are continuing to push ourselves to respond more rapidly and prevent attacks before they occur.

One area in which we have had great success with our overseas partners recently is in targeting infrastructure we believe has been used in Distributed Denial of Service

(DDOS) attacks, and preventing it from being used for future attacks. Since October 2012, the FBI and the Department of Homeland Security (DHS) have released nearly 168,000 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' National Cybersecurity and Communications Integration Center Team as well as our Legal Attachés.

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.

***Next Generation Cyber***

The need to prevent attacks is a key reason we have 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; establishing Cyber Task Forces in each of our 56 field offices to conduct cyber intrusion investigations and respond to significant cyber incidents; hiring additional computer scientists to assist with technical investigations in the field; and expanding partnerships and collaboration at the National Cyber Investigative Joint Task Force (NCIJTF).

At the NCIJTF – which serves as a coordination, integration, and information sharing center among 19 U.S. agencies and two foreign governments 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 National Security Agency (NSA), DHS, the Central Intelligence Agency, U.S. Secret Service, and U.S. Cyber Command. We recently invited our Five Eyes partners to join us at the NCIJTF. Australia agreed, and embedded personnel there in May. The U.K. is scheduled to do so in July 2013. By developing partnerships with these and other nations, NCIJTF is working to become the international leader in synchronizing and maximizing investigations of cyber adversaries.

We recognize that we must work together more efficiently than ever to keep pace with and surpass our cyber adversaries. To that end, the leaders of the FBI, DHS, and NSA recently held a series of meetings to clarify the lanes in the road in cyber jurisdiction. The group agreed that the Department of Justice (DOJ) is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DHS' primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. The Department of Defense's role is to defend the nation, gather intelligence on foreign cyber threats, and to protect national security systems.

Earlier this year, the U.S. Intellectual Property Enforcement Coordinator released the *Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets*. As part of the Strategy, the Department of Justice, including the FBI, will continue to prioritize prosecutions and investigations of foreign corporate and state-sponsored trade secret theft. Further, the FBI is expanding its efforts to fight computer intrusions that involve the theft of trade secrets by individuals, foreign corporations, and nation-state cyber hackers.

While we are primarily focused with our federal partners on cyber intrusions, we are also working with our state and local law enforcement partners to identify and address gaps in the investigation and prosecution of Internet fraud crimes.

Currently, the FBI's Internet Crime Complaint Center (IC3) collects reports from private industry and citizens about online fraud schemes, identifies emerging trends, and produces reports about them. The FBI investigates fraud schemes that are appropriate for federal prosecution (based on factors like the amount of loss). Others are packaged together and referred to state and local law enforcement. However, we have learned that very few of these referred cases are being worked.

To close this gap, we have developed a pilot program in collaboration with the International Association of Chiefs of Police, the Major City Chiefs Association, and the National Sheriff's Association to enhance the Internet fraud targeting packages IC3 provides to state and local law enforcement for investigation and potential prosecution. During the first phase of the pilot, IC3 will develop better investigative leads for direct dissemination to state and local agencies, beginning with the Utah Department of Public Safety.

### *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. We realize the flow of information must go both ways. As part of our enhanced private sector outreach, we have begun to provide industry partners with classified threat briefings and other information and tools to help them repel intruders.

Among them is a new platform we are developing for trusted private industry partners to report cyber incidents to us in real time. Known as iGuardian, it is based on the FBI's successful Guardian terrorist threat tracking and collaboration system.

Guardian has also been enhanced to accept cyber incident reporting from fusion centers and state and local law enforcement.

Over the past year, we have been engaged in classified briefs on nearly a daily basis at NCIJTF with private-sector partners and representatives of our nation's most critical infrastructure sectors. Earlier this year, in coordination with the Treasury Department, we provided a classified briefing on threats to the financial services industry to executives of more than 40 banks who participated via secure video teleconference in FBI field offices around the country.

In addition to these actions, we are also expanding our partnerships with private industry and academia through initiatives like InfraGard—a public-private coalition of 55,000 members to protect critical infrastructure—and the National Cyber-Forensics and Training Alliance, a proven model for sharing private sector information in collaboration with law enforcement.

### *FY-2014 Budget Request*

The combined result of these actions is that the FBI has undergone a paradigm shift over the past year in how we are responding to the cyber threat, particularly national security cyber threats. While we previously watched, collected information, and added to our understanding of our nation-state adversaries' intentions, we are now looking to disrupt and deter the individuals behind the keyboard who have made it their mission to attack, steal, spy, and commit terrorist attacks against our nation and its citizens.

Instead of watching foreign countries steal our intellectual property, we're going out to companies and trying to prevent it. For example, in coordination with DHS, we will provide organizations with IP addresses that are likely to launch attacks against them or the e-mail addresses used to send their employees messages with links to malicious software, in a technique known as "spearphishing."

Undertaking these new actions and initiatives requires additional personnel and other resources. That is why, to help the FBI combat this rapidly developing and diverse threat, the FY 2014 budget request includes an additional 152 positions (60 Special Agents, one Intelligence Analyst, and 91 Professional Staff) and $86.6 million to help address this threat.

### *Conclusion*

In conclusion, Chairwoman Mikulski, 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 as we determine a successful course forward for the nation to defeat our cyber adversaries.

Thank you again for the opportunity to be here today. I would be happy to answer any questions you may have.