Department of Justice

STATEMENT OF
JENNY A. DURKAN
UNITED STATES ATTORNEY
WESTERN DISTRICT OF WASHINGTON
DEPARTMENT OF JUSTICE

BEFORE THE
SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED:
"CYBER THREATS: LAW ENFORCEMENT AND PRIVATE SECTOR RESPONSES"

PRESENTED
MAY 8, 2013

Statement of
Jenny A. Durkan
United States Attorney
Western District of Washington
Department of Justice

Before the
Subcommittee on Crime and Terrorism
Committee on Judiciary
United States Senate

At a Hearing Entitled
"Cyber Threats: Law Enforcement and Private Sector Responses"
May 8, 2013

Good afternoon, Chairman Whitehouse, Ranking Member Graham, and Members of the Subcommittee. It is an honor to appear before you to testify about investigating and prosecuting cyber threats to our nation and the resources required to do so. I am pleased to share with the Subcommittee an overview of the Department of Justice's role in the U.S. Government's overall investigative strategy and enforcement efforts as it relates to cyber. The President's 2014 budget also has some funding requests that would enhance our ability to address these threats. I will provide more detail later in my remarks. The Department's approach to 21st Century cyber threats is rooted in three interests: 1) deterring, disrupting, and dismantling the threat; 2) holding bad actors accountable; and 3) protecting our national security, economic interests, and individual privacy.

As United States Attorney, I see the full range of threats our communities and nation face. Few things are as sobering as the daily cyber threat briefing I receive. Cyberspace is the new frontier. We have witnessed the rapid creation of incredible businesses, lifesaving technologies, and new ways to connect society. Unfortunately, the "good guys" are not the only innovators. We have seen a significant growth in the number and nature of bad actors exploiting new technology. As Attorney General Holder has noted, "[f]rom criminal syndicates, to terrorist organizations, to foreign intelligence groups, to disgruntled employees and other malicious intruders, the range of entities that stand ready to execute and exploit cyber attacks has never been greater." Threats to the nation's computer networks and cyber systems continue to evolve, as the nature and capabilities of those responsible for the threats evolve. Over the last several years, investigators and prosecutors have seen significant increases in the skills of threat actors and the complexity of their organizations. These actors have a variety of aims and motivations. For instance:

- Financially motivated groups working closely and easily across national boundaries have stolen large quantities of personal data. These criminals coalesce in forums where they barter individual skills to create ad hoc criminal networks with a power and reach sometimes approaching that of traditional transnational organized crime networks.

- Criminal groups have also developed tools and techniques for disrupting and sometimes damaging computer systems. Motivations run from profit to politics, but their motivations do not change the damage incurred by users and our economy.

- State actors and organized criminal groups have demonstrated the desire and the capability to steal sensitive data, trade secrets, and intellectual property for military and competitive advantage. Whether through remote attacks or insider threats, such thefts pose significant risk to our national security and economic interests.

- Malicious actors are now seeking to exploit the computer networks that control our critical infrastructure.

Responding to these threats requires a multi-faceted approach, including diplomacy and public-private partnerships. The Department, acting with its law enforcement components and in partnership with other agencies, plays a critical role by identifying the offenders, seizing their hardware and assets, and deterring their conduct through, among other things, indictment, arrest, prosecution, and appropriate punishment. In doing so, the Department works closely with other agencies and private sector entities to reduce vulnerabilities. Stated another way, we need to develop better locks, but when those locks are broken—as they inevitably will be—the Department responds to bring the offenders to justice.

Our reliance on technology requires that we take action to protect not only the information infrastructure itself, but the data it carries and activity that it supports. The Administration is committed to integrating and organizing the government's cybersecurity efforts to better ensure that we have a comprehensive framework in place that will allow us to bring all of our collective tools to bear in the fight against cyber criminals, terrorists, and other adversaries. The Department of Justice plays a key role in that fight.

Nature of the Threat

Ten years ago, many of the threats to the burgeoning Internet came from solo hackers, writing viruses like "I love you" or "Melissa," or crafting denial of service attacks on fledgling Internet companies. As bothersome as those attacks were, the threats today are much more significant. We face the challenges of organized crime, botnets (i.e., a collection of compromised computers under the remote command and control of a criminal or foreign adversary), identity theft, and carding, to name just a few. Many of these threats originate overseas.

However, we face significant challenges in attributing the origin of these threats. The tools used to commit serious cyber theft and damage are not only wielded by those with large-scale development resources. Instead, using widely available tools, individuals or small groups can steal huge quantities of sensitive data, damage key computer systems, or silence those who

disagree. Financial gains from these crimes can, in turn, be used to build larger networks and buy protection from foreign government officials. As a result, U.S. investigators working to determine the source and nature of a cyber threat often do not know at the outset whether an attack was mounted by an individual acting alone, an organized criminal or terrorist group, or a hostile nation.

Every day, criminals hunt for our personal and financial data so that they can use it to commit fraud or sell it to other criminals. The technology revolution has facilitated these activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled criminal hackers are now able to perpetrate large-scale data breaches that leave hundreds of thousands—and in many cases, tens of millions—of individuals at risk of identity theft. Today's criminals can remotely access the computer systems of universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including financial information. As I explain below, we are working hard to address these threats to personal information.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A 2011 report from McAfee and Science Applications International Corporation confirms this trend in cybercrime. According to this report, which was based on a survey of more than 1,000 senior IT decision makers in several countries, "high-end" cyber criminals have shifted from targeting credit cards and other personal data to the intellectual capital of large corporations. This includes extremely valuable trade secrets and product-planning documents.

These threats come both from outside criminal hackers as well as insiders who gain access to critical information from within companies and government agencies. Trusted insiders pose particular risks. Those inside U.S. corporations and agencies may exploit their access to funnel information to criminals, competitors or foreign nation states. And once the enemy is inside the gates, external defense can only provide limited protection. The Justice Department has successfully prosecuted corporate insiders and others who have obtained trade secrets or technical data from major U.S. companies and routed them to other nations via cyberspace.

The massive proceeds from these online crimes create another troubling issue. It is too soon to say where that money ends up, but the risk that it is being used to influence foreign governments, distort foreign justice systems, and fund terrorists cannot be ignored.

The national security cyber threat picture has similarly undergone a dramatic evolution in recent years. Although we have not yet experienced a devastating cyber attack against our critical infrastructure, we have been victim to a range of cyber activities that have siphoned off our valuable economic assets or had other effects on our infrastructure, threatening our nation's security.

These threats are as varied as the actors who carry them out. While details about most of the state-sponsored intrusions remain classified, the Intelligence Community has publicly noted that "entities within China and Russia are responsible for extensive illicit intrusions into US computer networks and theft of US intellectual property." Indeed, "Chinese actors are,"

according to a 2011 public report of our top counterintelligence officials, "the world's most active and persistent perpetrators of economic espionage." The Secretary of Defense has stated that "Iran has also undertaken a concerted effort to use cyberspace to its advantage."

Likewise, the threat of cyber-enabled terrorism looms large. While terrorists have not yet used the Internet to launch a full-scale cyber attack against the United States, they already use cyberspace for more than merely spreading propaganda and recruiting followers – they have used cyberspace to facilitate operations. The individuals who planned the attempted Times Square bombing in May 2010, for instance, used public web cameras for reconnaissance, file sharing sites to share operational details, and remote conferencing software to communicate. In addition, they have exhorted their followers to engage in cyber attacks on America. Last year, an al-Qaeda video released publicly by the Senate Homeland Security Committee encouraged al-Qaeda followers to engage in "electronic jihad" by carrying out cyber attacks against the West.

The national security cyber threats posed by state-sponsored actors and terrorists are growing, and although to date they have resembled in some ways the crimes perpetrated by financially-motivated criminals, their emergence and evolution make the threat of cyber-generated physical attacks, like those that might disrupt the power grid, appear no longer to be the stuff of science fiction. Leaders in our national security community have predicted that the cyber threat "will pose the number one threat to our country" in "the not too distant future." Accordingly, just as the Department realigned its counterterrorism efforts after 9/11, we are realigning our cyber efforts to meet this challenge.

Addressing these complex threats requires a unified approach, one that incorporates criminal investigative and prosecutorial tools, civil and national security authorities, diplomatic tools, public-private partnerships, and international cooperation. Criminal prosecution, whether in the United States or a partner country, plays a central and critical role in this collaborative effort. While prosecution is not the appropriate approach for every threat that affects the United States, identifying and understanding the threat will very often involve the use of criminal investigative tools and methods.

Role of the Department of Justice

A key part of the nation's overall cybersecurity effort is the investigation and prosecution of cyber criminals – be they financially motivated actors, criminal hackers, terrorists, or state actors. Our goal is to stop or deter these actors before they can complete an attack on our networks, or to punish and deter similar acts in the future if a successful intrusion has already occurred. Many Department of Justice components—including the Criminal and National Security Divisions and United States Attorneys' offices across the country—are actively working to counter these threats.

These cases can be complex to investigate and prosecute. We need to ensure we have the investigative expertise and forensic capabilities needed to meet the challenge. We appreciate the support this committee has given in this regard. Almost every federal case prosecuted now

involves an increasing volume of digital evidence, sometime scattered over numerous devices and multiple online services. For example, in one recent case in our District, the target carried as many as 15 cell phones. Gathering, sifting, and analyzing digital evidence is an increasing challenge. Bad actors know how to hide their cyber tracks: evidence can disappear with a few key strokes, or through malicious code set as a booby trap. Moreover, large cyber cases frequently involve multiple players in multiple states and countries. One significant case can require multiple agents and several years to investigate. Obtaining evidence from foreign countries – even those that are strong allies – can take time, delay, and require translating voluminous foreign language evidence.

To meet these challenges, the Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cybercrime wherever it occurs. The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and a nationwide network of Assistant United States Attorneys (AUSAs), including nearly 300 AUSAs designated as Computer Hacking and Intellectual Property (CHIP) prosecutors lead our efforts to investigate and prosecute cybercrime offenses. These prosecutors, as well as other Assistant United States Attorneys (AUSAs) working cybercrime cases throughout the country, work closely with our law enforcement partners, including the FBI, the Secret Service, and the U.S. Postal Inspection Service. In addition, we have a strong partnership with the FBI's National Cyber Investigative Joint Task Force (NCIJTF), which brings together law enforcement, intelligence, and defense agencies to focus on high-priority cyber threats.

Other sections of the Criminal Division also play important roles in cybersecurity. The Fraud Section focuses on large-scale fraud cases involving identity theft. The Office of International Affairs (OIA) supports and enhances international cooperation efforts by expediting the sharing of critical electronic evidence with foreign law enforcement partners and by marshaling efforts to secure the extradition of international fugitives. Increasingly, large scale cyber cases involve actors from any number of foreign countries. OIA not only secures evidence and international fugitives from abroad, it also plays a central role in cultivating law enforcement cooperation with foreign partners by complying with the United States' reciprocal obligations to provide U.S.-based evidence to foreign authorities for their investigations. International cooperation is critical and the work of OIA a key component of our success.

The Department's National Security Division (NSD) pursues national security cyber threats through a variety of means, including through counterespionage and counterterrorism investigations and prosecutions. The Counterespionage Section (CES) prosecutes, among other offenses, misappropriation of intellectual property to benefit a foreign government, as provided by the Economic Espionage Act of 1996 (18 U.S.C. § 1831), and obtaining national defense, foreign relations, or restricted data by accessing a computer without authorization, as provided by the Computer Fraud and Abuse Act (18 U.S.C. § 1030). The Counterterrorism Section (CTS)—leveraging the capabilities and expertise of CCIPS, the Anti-Terrorism Advisory Council, Joint Terrorism Task Forces, and others—would play a pivotal role in addressing any potential cybersecurity attack by terrorists or associated groups or individuals. NSD also

provides the FBI, and the intelligence community in general, with extensive legal support on cyber issues.

Recognizing the diversity of national security cyber threats and the need for a coordinated approach to them, the Department also established last year a nationwide network of National Security Cyber Specialists (referred to as the "NSCS network"). The network brings together the Department's full range of expertise on national security-related cyber matters, drawing on experts from NSD, the U.S. Attorney's Offices, CCIPS, and other DOJ components. This network seeks to build on the successes of existing initiatives, including the CHIP network and the Anti-Terrorism Advisory Council. Each U.S. Attorney's office around the country has designated a point of contact for the National Security Cyber Specialists network. Last year, approximately 120 Assistant U.S. Attorneys and presenters convened in Washington, D.C. for a cyber training program to kick off the NSCS program.

The NSCS network now serves as a centralized resource for prosecutors and agents around the country. The network has focused the Department nationwide on opening more national security cyber investigations with an eye toward criminal prosecution. Through this network, we are bringing our best resources to bear against the problem—to enhance information sharing, ensure coordination, and leverage the Department's expertise in legal authorities and advice relating to national security cyber threats. Finally, we are using this network to do more outreach to the private sector and to enhance our joint work with the NCIJTF.

In addition to these efforts, the Department works closely with our partners throughout the government—including law enforcement agencies, the Intelligence Community, the Department of Homeland Security (DHS), Department of Commerce, and the Department of Defense—to provide legal support to cybersecurity efforts and inform policy discussions. The intersection between laws and technology can require complicated analysis and multidisciplinary training. That is why the Department has lawyers in US Attorneys offices, and the Criminal and National Security Divisions, who are specially trained to handle cyber issues, ranging from the use of existing legal tools and authorities, the legality of cybersecurity programs like the EINSTEIN program, and the ways in which we can vigorously protect privacy, confidentiality, and civil liberties while still achieving our goal of securing the Nation's networks. Partnering with the National Science Foundation (NSF), through NSF's CyberCorps Scholarship for Service (SFS) program - which seeks to increase the number of qualified students entering the fields of information assurance and computer security and to increase the capacity of the U.S. higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society – the Department currently employs more than 40 SFS CyberCorps graduates, including 17 working for the Federal Bureau of Investigation.

For example, the Department is currently providing legal and policy advice to the Department of Homeland Security in support of its cybersecurity mission and to the National Security Agency in support of its information assurance efforts. We are participating in government-wide planning and preparedness efforts, such as the development of the National Cyber Incident Response Plan and the associated Cyber Unified Coordination Group, which assists the Secretary of DHS in coordinating responsive measures to significant cyber incidents. We also participate

in cyber exercises, such as 2012's National Level Exercise, and, along with other governmental partners, in reviewing the national security implications and vulnerabilities of certain foreign acquisitions of U.S. companies, including those with cyber-related capabilities.

Our work does not stop at our shores. Due to the global nature of the Internet, many of our cases involve computers and electronic evidence located in other countries. Many times the offenders are located in another country. Even U.S. criminals will use computers located in another country to hide their tracks. Often it is impossible to identify, arrest, and prosecute offenders without the assistance of foreign governments.

To assist us in preserving and obtaining evidence from other nations, the Department, with funding support from the Department of State Bureau for International Narcotics and Law Enforcement Affairs, has engaged in numerous efforts to enhance the ability of foreign governments to fight cybercrime, including:

- promoting the Council of Europe Convention on Cybercrime (2001);
- providing technical expertise to countries developing their legal frameworks relating to computer crime and electronic evidence;
- providing U.S.-based evidence through mutual legal assistance treaties to aid foreign investigations;
- providing capacity building assistance for foreign law enforcement agencies; and
- promoting the 24/7 High-Tech Crimes Network of the G8, which is a network of points of contact designed to facilitate rapid law enforcement coordination across borders.

The profusion and diversity of cyber threats, and the challenges inherent in identifying and addressing them, highlight the need for a whole-of-government approach—an all-tools approach—to combating cyber threats. As Director Mueller has said, "We must be willing to use whatever legal means are available and appropriate—civil, criminal, or other means—to disrupt a particular threat—whether it be a terrorist threat or a cyber threat."[1] Just as law enforcement and other legal tools have been critical in our efforts to combat organized crime, terrorist threats, and espionage, so too will they be critical to the deterrence and disruption of cyber threats.

Operational Successes

The relationships between the Department's prosecuting components and the federal investigative agencies, such as the U.S. Secret Service and the Federal Bureau of Investigation, and the robust cooperation and information sharing that they support, have led to a number of

[1]Address at RSA Cyber Security Conference, San Francisco, CA (February 28, 2013) http://www.fbi.gov/news/speeches/working-together-to-defeat-cyber-threats.

enforcement successes. In FY 2012, computer intrusion investigations resulted in 138 convictions and pre-trial diversions. I would like to highlight a few here.

International, Multi-state Carding Ring – In my District, we prosecuted participants at all levels of an international credit card skimming ring from a Secret Service investigation. Christopher A. Schroebel, 21, of Keedysville, Maryland, obtained credit card information by hacking into vulnerable point of sale computers in small business operations across the country, including one in the Seattle area. Tens of thousands of people were victimized, and the investigation indicated that over 100,000 credit cards were compromised. David Benjamin Schrooten, 22, a Dutch citizen living in Romania sold the card numbers for a profit by advertising them on "carding websites." Charles Tony Williamson, 33, of Torrance, California, has also been charged with buying the card numbers for his criminal group to use in multiple frauds. Schroebel was sentenced to seven years in prison, Schrooten received a twelve year sentence, and Williamson is awaiting trial.

Prolific Identity Thief and Hacker Sentenced. Following a complex Secret Service investigation, on July 18, 2012, a court in the Eastern District of New York sentenced Aleksandr Suvorov to seven years in prison following his 2009 plea to conspiracy to commit wire fraud and his 2011 plea to trafficking in unauthorized access devices. Suvorov, an Estonian, was extradited from Germany in 2009. Along with Albert Gonzalez and Maksym Yastremskiy, he participated in a massive hacking scheme involving retail merchants. The May 2009 pleas, for example, involved a hack into the Dave & Buster's restaurant chain in which the group stole names and account numbers for approximately 110,000 credit card accounts. Gonzalez, arguably the most prolific identity thief in American history, had already pled guilty and was sentenced in March 2010 to 20 years in prison. Yastremskiy earlier received a 30-year prison term in Turkey for identity theft and related crimes.

Coreflood Botnet Takedown. In April 2011, the government filed a civil complaint against 13 "John Doe" defendants, alleging that they ran the Coreflood Botnet in order to engage in wire fraud, bank fraud, and illegal interception of electronic communications. At its peak, the group had control over several million computers infected with the Coreflood malware. Search warrants were obtained for computer servers throughout the country, and a seizure warrant was obtained for 29 domain names. The government also obtained a temporary restraining order (later followed by a preliminary and permanent injunction), authorizing the government to respond to signals sent from infected computers in the U.S. in order to stop the Coreflood software from running, thereby preventing further harm to hundreds of thousands of unsuspecting users of infected computers in the United States. Over the next month, the Coreflood Botnet was effectively eliminated.

Charges Brought Against Six Leaders of Anonymous and Related Criminal Hacking Collectives. In March 2012, the Southern District of New York (SDNY) unsealed charges against five criminal computer hackers in the United States and abroad

who identified themselves as aligned with the online group "Anonymous" and/or related offshoot groups including "Internet Feds," "LulzSec," and "AntiSec." SDNY unsealed one indictment that charged Ryan Ackroyd, aka "kayla"; Jake Davis, aka "topiary,"; Darren Martyn, aka "pwnsauce,"; and Donncha O'Cearrbhail, aka "palladium," with computer hacking conspiracy involving the hacks of Fox Broadcasting Company, Sony Pictures Entertainment, and the Public Broadcasting Service (PBS), among others. In addition, SDNY unsealed the guilty plea of Hector Xavier Monsegur, aka "Sabu," the former head of Anonymous and LulzSec who had been cooperating with the FBI since his arrest in the Southern District of New York in June 2011. Monsegur pleaded guilty not only to charges in SDNY, but also to substantive hacking charges filed by four other U.S. Attorney's Offices -- Eastern District of California (hacks of HBGary, Inc. and HBGary Federal LLC), Central District of California (hacks of Sony Pictures Entertainment and Fox Broadcasting Company) , Northern District of Georgia (hack of Infraguard Members Alliance), and Eastern District of Virginia (hack of PBS). Finally, the FBI arrested Jeremy Hammond, aka "Anarchaos," who identified himself as a member of "AntiSec," on a complaint in SDNY that charged him in connection with the hack of Stratfor, a global intelligence firm based in Austin, Texas.

Notorious Criminal Hacker and Identity Thief Surrendered by France to the U.S. On April 5, 2013, Vladislav Anatolievich Horohorin, a/k/a "BadB" was sentenced to 88 months in prison by Judge Huvelle in the District Court for the District of Columbia. Horohorin, a citizen of Russia, Ukraine, and Israel, was a major vendor of stolen credit and debit cards who possessed more than 2.5 million stolen account numbers at the time of his arrest. Horohorin also participated in the intrusion at Atlanta-based RBS Worldpay in 2008, in which an international criminal group that completed more than 15,000 fraudulent transactions at over 2,100 ATMs in at least 280 cities worldwide in a 12-hour period in November 2008, causing more than $9.4 million in losses. Horohorin was extradited to the United States from France, where he was arrested on August 8, 2010 at the request of U.S. authorities.

Romanian "Point-of-Sales" Criminal Hackers Extradited to U.S. Following an extensive Secret Service investigation, on May 4, 2011, a federal grand jury in Concord, New Hampshire, returned an indictment charging Adrian-Tiberiu Oprea, Cezar Iulian Butu, Iulian Dolan, and Florin Radu, all residents of Romania, with conspiracy to commit computer intrusions, wire fraud, and access device fraud. The defendants were part of a group that, beginning in 2008, remotely hacked into Subways' and other merchants' "checkout" or "point-of-sales" computer systems; surreptitiously installed "keystroke logging" software, which in turn recorded and stored customers' credit, debit, and gift card data; electronically transferred the stolen card data to several U.S.-based computer servers ("dump sites") and from there to a server in Cyprus, for temporary storage; and then made unauthorized charges on the compromised accounts and sold stolen card data to other co-conspirators. Members of the conspiracy have compromised over 146,000 accounts and have made unauthorized charges in excess of $10,000,000 on these compromised accounts. Dolan and Butu, were arrested upon their entry to the United

States in August 2011, have pled guilty, and remain in United States custody awaiting sentencing. Adrian-Tiberiu Oprea, 28, of Constanta, Romania, was extradited from Romania to the United States and appeared in federal court in New Hampshire on May 29, 2012. Radu is currently at large.

Operator of Worldwide Spam Botnet Convicted. On February 27, 2013, Oleg Nikolaenko, 25, a citizen of Russia who entered the United States on a tourist visa, was sentenced to time served (just over 27 months) in the Eastern District of Wisconsin following an earlier guilty plea. According to court documents, Nikolaenko operated and controlled the Mega-D botnet, which was at one time the world's largest spam botnet, accounting for approximately 32% of all spam worldwide. A network security company estimates that approximately 509,000 computers worldwide were infected with Mega-D botnet malware.

Operation Trident Tribunal Takes Down International Crime Rings Distributing Scareware. Operation Trident Tribunal is a coordinated international enforcement action targeting a cybercrime ring that caused over $71 million in losses to more than one million computer users by operating a "scareware" scheme. Scareware is malicious software that cybercriminals plant on victim computers through a variety of computer exploits including the use of botnets, "drive-by" downloads, and criminal search engine manipulation. The scheme uses a variety of ruses, including web pages featuring fake computer scans, to trick consumers into purchasing fake anti-virus software products at a cost of up to $129. In June 2011, DOJ coordinated the efforts of law enforcement in over a dozen countries to seize dozens of servers that were being used to orchestrate this scheme. Two Latvian nationals, four Ukrainian nationals, and a Swedish national were indicted in connection with the scheme, and five foreign bank accounts were frozen.

On January 19, 2012, defendant Mikael Patrick Sallnert, a citizen of Sweden, was arrested in Denmark and extradited to the United States. Sallnert was a trusted payments processor for the scareware ring, responsible for processing funds fraudulently obtained from U.S. victims. Sallnert pleaded guilty to one count of conspiracy to commit wire fraud and one count of accessing a protected computer in furtherance of fraud on August 17, 2012, and was sentenced to 48 months in prison on December 14, 2012 by Judge Pechman in the Western District of Washington.

These cases illustrate the broad scope of the Department's efforts to pursue cyber criminals. While the Department is proud of these cases and all of our efforts to tackle the growing and evolving cybersecurity problem, we recognize that there is much more to be done, and we will continue to work with our law enforcement and private sector partners to meet that challenge. Because of the global nature of the Internet and the related crimes it can facilitate, continued close coordination and cooperation with foreign law enforcement is critical to our collective success. And because our prosecutors understand the severe damage that computer crimes can have upon a victim, we continue to pursue appropriate cases, both large and small.

Legislation to Enhance the Department's Ability to Combat Cyber Threats

As the threat increases and evolves, so must our legal tools to combat the threat. In May 2011, as part of the Administration's Cybersecurity Proposal, the Department proposed some needed, moderate updates to the computer crime laws.2 We continue to believe that many of these proposals would enhance our ability to combat cyber threats, including:

- A proposal to update the Racketeering Influenced and Corrupt Organizations Act ("RICO") to make the Computer Fraud and Abuse Act ("CFAA") offenses subject to RICO. The CFAA is the primary statute used to prosecute hacking crimes. Computer technology has become a key tool of organized crime. Indeed, criminal organizations are operating today around the world to: hack into public and private computer systems, including systems key to national security and defense; hijack computers for the purpose of stealing identity and financial information; extort lawful businesses with threats to disrupt computers; and commit a range of other cybercrimes. Many of these criminal organizations are similarly tied to traditional Asian and Eastern European organized crime organizations.

- A proposal to clarify and update the forfeiture provision of the CFAA. This proposal would allow for civil forfeiture and clarify the rules governing criminal forfeiture under the statute.

- A proposal to update the CFAA's sentencing provisions. The goal of these changes is to eliminate overly complex, confusing provisions; simplify the sentencing scheme; and enhance penalties in certain areas where the statutory maximums no longer reflect the severity of these crimes.

Resources to Enhance the Department's Ability to Combat Cyber Threats

Because of the very serious nature of cyber threats, and the pressing need to respond to them, the Administration is asking for an enhancement to the Department's budget to target this critical problem. These additional resources will help us to keep pace with the increased numbers and ever evolving sophistication of our adversaries. The Department's FY 2014 Budget proposal therefore provides a total of $668 million in cyber resources to address computer intrusions and cybercrimes and to defend the security of the Department's critical information networks. This request includes an increase of $92.6 million for the FBI, NSD, and the Criminal Division.

For the FBI, the budget includes an increase of $86.6 million and 152 positions (60 agents) to support the FBI's Next Generation Cyber Initiative, which will more strategically focus the FBI's efforts on the greatest cyber threat—intrusions into government and industry computer networks. The Next Generation Cyber Initiative combines national security and criminal

[2] *See* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security.pdf.

investigative resources to more holistically approach multi-dimensional cybercrimes and to better leverage the full range of FBI authorities. The requested funding will add 50 special agents and 50 computer scientists to increase cyber investigative capabilities and victim notification, enhance the capabilities and expertise of FBI investigative personnel, and improve the collection and analysis of electronic evidence. It will also extend centralized analytical capabilities to the field by deploying cyber workstations to serve as portals for communicating intrusion-related data bureau-wide.

Like the FBI, the Department's National Security Division seeks to improve its capability to respond to cyber-based threats to the national security and the capability to respond. Cyber-based threats to the national security are, according to the intelligence community "increasing in scope and scale," and cyber-espionage in particular "is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena." NSD is involved in the full range of U.S. cyber and cyber security efforts, including cyber threat prevention, detection, disruption, investigation and prosecution, as well as oversight, vulnerability management, and cyber policy development. As I mentioned above, last year NSD created the National Security Cyber Specialists Network to facilitate a threat-based approach, rather than a statute- or tool-based approach, to the national security cyber challenge. To this end, NSD is establishing "threat focus" cells of cyber specialists to focus on particular high-priority cyber targets. The subject-matter experts who comprise such teams will serve as Departmental focal points for information about—and strategies designed to defeat—these identified cyber threats. One such cell has already been created, and has successfully begun work on a significant threat actor.

As NSD positions itself to better accomplish its cyber mission, and as it continues its work leading, expanding, and developing the NSCS Network, our first priority is ensuring that we have a well-equipped cyber workforce. To achieve this goal, NSD must hire, equip, and train both new and existing personnel. These additional resources are critical to ensuring that the Division's redoubled cyber efforts do not detract from ongoing, and critical, counterterrorism, counterespionage, and intelligence-related matters. As a result, NSD has requested $3.5 million and 26 positions (16 attorneys) for FY14. This increase will enable NSD to strengthen its investigative, prosecutorial, intelligence collection, and oversight abilities to support the Intelligence Community in identifying and disrupting cyber threats to national security.

Similarly, the Criminal Division has seen a growth in cyber threats perpetrated by actors other than foreign nation states and terrorist organizations. And as I mentioned before, criminal prosecution, whether in the United States or a partner country, plays a central and critical role in eliminating these threats. In addition, while prosecution is not the appropriate approach for every threat that affects the United States, identifying and understanding the threat will very often involve the use of criminal investigative tools and methods. Just as the threats to our nation's invaluable proprietary and personal information are increasing, so must our innovation and our efforts to deter, disrupt, and prosecute those threat actors. Studies have shown that the number of intrusions continues to increase, and the cost of cybercrime to American businesses and citizens likewise continues to mount. The Division's Computer Crime and Intellectual

Property Section (CCIPS) has experienced a 42% increase in pending investigations and an 11% increase in pending prosecutions between FY 2010 and FY 2011. The requested additional resources will help the Division keep pace with the growing cyber caseload and should be viewed in tandem with the increase in FBI investigative resources for FY 2014.

A reality of cyber investigations is that it is nearly impossible to forecast where they will begin or end. Consequently, the Division, through CCIPS, provides nation-wide support to investigations, prosecutions, and disruption efforts, helping to ensure that its law enforcement partners receive consistent, quality support whether the investigation's trail leads to Silicon Valley, rural America, or overseas. As a result, Criminal Division prosecutors have led, or partnered in, some of the country's most significant data breach and computer intrusion cases, the success of which has required a comprehensive grasp of computer network technology and electronic evidence law and a subtle understanding of the often loosely organized worldwide groups that work together to plan and execute these attacks.

CCIPS prosecutors work in direct cooperation with the CHIP network and investigative agencies to identify and address threat actors. CCIPS houses prosecutors with a deep understanding of data breaches and computer misuse cases and prosecutors who understand the complexity of intellectual property cases to comprise a leading resource for deterring, investigating, and punishing the theft of sensitive electronic information. Consequently, every additional prosecutor in CCIPS becomes a force multiplier for the Department, leveraging its expertise wherever it is needed to the benefit of all USAOs and the achievement of the Department's cyber crime goals.

The Criminal Division is therefore requesting an increase of 25 positions (9 attorneys), 14 FTE, and $2,580,000. This enhancement will increase the Division's capability in four key areas: cybercrime investigations and prosecutions; advice to the field regarding legal tools and authorities; international cooperation and outreach; and forensic support. This increased capacity will allow the Division to successfully deter, investigate, and punish the theft of sensitive electronic information and other cybercrime.

Moreover, a critical part of the Department's efforts to combat cyber threats is international engagement. As I have just described, criminals residing outside of our borders are a major component of the overall threat, and even criminals inside the U.S. commonly use computers overseas to store their tools, hide stolen data, and conceal their identities. Thus, a critical part of addressing the cyber threat is to improve our ability to work with law enforcement agencies in foreign governments to collect electronic evidence on our behalf and arrest and either extradite or prosecute cyber criminals.

The Criminal Division has long had a robust program for encouraging the development by foreign governments of laws, investigation and prosecution capacity, and appropriate infrastructure to address emerging cybercrime threats and capabilities. From the development and maintenance of a 24/7 response capability in more than 50 countries aimed at preserving critical evidence before it is deleted, to its leading role in negotiating the first multilateral convention on cybercrime, to its regular engagement on training, policy, and operational issues

with law enforcement partners around the world, the Division and its partners in the US Attorneys offices have led the fight against transnational cybercrime.

Despite significant advances in law enforcement cooperation and understanding, criminals continue to use gaps and inefficiencies in international law enforcement capabilities to evade detection, attribution, and punishment. Foreign authorities apply data protection regulations in ways that can frustrate investigations. Delays in evidence collection can stop investigations almost at their inception. And some of the myriad entities involved in providing Internet connectivity and domain registration have permitted the growth of "data havens" where criminal and other threat actors can commit crimes with relative impunity.

Despite these challenges, the Criminal Division has attempted to perform effective international outreach on cyber issues. Using a balanced approach of frank policy discussions with countries that have similar capabilities, combined with multilateral training initiatives aimed at countries whose legal or technical infrastructure to address cyber threats is at an earlier developmental stage, the Division has continued to improve capacity to address cybercrime around the world. CCIPS attorneys lead efforts to build capacity and law enforcement relationships in Africa, Eastern Europe, and Latin America, including through multi-lateral organizations such as the Organization of American States and the Asia-Pacific Economic Cooperation. As computer infrastructures expand in developing countries, and offenders who victimize Americans inevitably follow, the need for this sort of international engagement continues to grow.

Having prosecutors stationed in foreign hotspots will contribute immeasurably to these efforts. Consequently, the Criminal Division also requests an enhancement of 11 positions (including 7 attorneys), 6 FTE, and $3,500,000 to place four DOJ Attachés overseas. These DOJ Attachés will serve as regional International Computer Hacking and Intellectual Property coordinators (ICHIPs). This program will build on the existing Intellectual Property Law Enforcement Coordinator Program (IPLEC) that has proven to be very effective in enhancing the Department's goals in fighting international intellectual property crime. Since 2006, the IPLEC Program has deployed experienced federal prosecutors overseas to take the lead on our intellectual property protection efforts in key regions including Asia and, until March 2011 (when State Department funding expired), Eastern Europe. Through the IPLEC program, the Department has seen a substantial increase in foreign enforcement and cooperative casework where U.S. law enforcement has had a visible and ongoing presence in the most active countries or regions. This enhancement request would allow for the expansion of the program to additional critical regions.

* * *

The Department of Justice stands ready to work with the Committee as it examines these important issues. We appreciate the opportunity to testify today, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.