Department of Justice

STATEMENT OF

JASON WEINSTEIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE
CRIME AND TERRORISM SUBCOMMITTEE

ENTITLED

"CYBERSECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM"

PRESENTED

April 12, 2011

Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and Members of the Subcommittee. It is a pleasure to appear before you to testify about ensuring our nation's cybersecurity. I am pleased to share with the Subcommittee an overview of the Department of Justice's role in the U.S. Government's overall cybersecurity strategy and enforcement efforts. In light of the FBI's participation on the panel, I will limit my remarks primarily to the ways in which other components of the Justice Department address cybersecurity issues.

Our society's reliance on digital infrastructure requires that not only the information infrastructure itself, but also all of the data it carries and activity that it supports be protected. 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 appropriate tools to bear against cyber criminals, terrorists, and other malicious actors. The Department of Justice plays a key role in that fight.

As the Administration's 60-Day Cyber Policy Review recognized, the Department, through its prosecutorial and law enforcement components, and in partnership with other agencies, plays a critical role in cybersecurity by identifying the offenders, seizing their hardware and assets, and deterring their conduct through arrest and appropriately severe punishment. Its role in threat reduction and attribution works in concert with the roles of other agencies and private sector entities that focus on hardening targets and reducing 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.

Nature of the threat

As you know, the United States depends upon the information and communications infrastructure to conduct commercial, financial, personal, and governmental transactions. We face ongoing threats to the security of that infrastructure from a wide range of actors, including nation-states, criminals, and terrorists who exploit our pervasive dependency on information technology to misappropriate or destroy information, steal money, and threaten basic services, including those provided by critical infrastructures.

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 troubling as those attacks were, the threats today are much more significant. We face the challenges of organized crime, botnets, identity theft, and carding, to name just a few. Many of these threats are based or originate overseas.

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 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 government agencies, universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including personal financial information.

Online threats may take many forms, including "carders" and "phishers." "Carding" encompasses not only the unauthorized use of credit and debit card account information to fraudulently purchase goods and services, but also a growing assortment of related activities including computer hacking, phishing, cashing out stolen debit card numbers, re-shipping schemes, and Internet auction fraud. Through carding activity, which has become a growing problem in recent years, large volumes of data are stolen, resold, and ultimately used by criminals to commit fraud.

"Phishing" refers to an email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Carders and phishers, among other types of cyber criminals, comprise a criminal underground in the cyber world that is dedicated to stealing and exploiting identity and financial information. Many of the actors in this criminal underground are outside of our national borders.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A report just released by 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 hackers as well as insiders who gain access to critical information from within companies and government agencies.

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 could be used to influence foreign governments, distort foreign justice systems, and fund terrorists cannot be ignored.

Let me give you an example of the kind of criminals that we are up against: organized, international, and profit-driven. In October 2009, nearly 100 people were charged in the U.S. and Egypt as part of an operation known as Phish Phry—one of the largest cyber fraud phishing cases to date and the first joint cyber investigation between Egypt and the United States. Phish Phry was the latest action in what Director Mueller described as a "cyber arms race" where law enforcement must coordinate and collaborate in order to keep up with its cyber adversaries. The defendants in Operation Phish Phry targeted U.S. banks and victimized hundreds of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled. More than 50 individuals in California, Nevada, and North Carolina and nearly 50 Egyptian citizens have been charged with crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identity theft. Led by the

FBI, this investigation required close coordination with state and local law enforcement, the Secret Service, and our Egyptian counterparts. In late March, five more people were convicted of federal charges for their roles in this "phishing" operation, bringing the total number of convictions to date to 46.

Role of the Department of Justice

The Department works closely with our partners throughout the government—including law enforcement agencies, the Intelligence Community, the Department of State, the Department of Homeland Security (DHS), and the Department of Defense—to provide legal support to cybersecurity efforts, inform policy discussions and ensure coordination of international efforts. The intersection between laws and technology can require complicated analysis and multidisciplinary training. That is why the Department has criminal lawyers, as well as attorneys working on national security matters, who are specially trained to handle cyber issues, ranging from the use of existing legal tools and authorities, to the ways in which we can vigorously protect privacy and civil liberties while still achieving our goal of securing the Nation's cyberspace.

Our work does not stop at our shores. Due to the global nature of the Internet, many of our cases involve computers located in other countries. Many times the offenders are located in another country. But 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. Due to the transnational nature of most cybersecurity incidents, achieving effective multilateral cooperation in real time has become a priority, which in turn has meant a higher priority for Department participation in US government delegations to various international bodies.

To assist us in preserving and obtaining data from other nations, the Department has engaged in numerous efforts to help address cybercrime problems around the world, including:

- promoting the Budapest Convention (Council of Europe Convention on Cybercrime), to which the U.S. is a party, and
- using State Department Foreign Assistance funds to provide capacity-building training and technical assistance to developing countries, including advice on developing their legal frameworks in this area, 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.

In the interagency context, the Department is currently providing legal and policy support to the Department of Homeland Security in support of its cybersecurity mission and 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, and cyber exercises such as Cyber Storm III.

Finally, the Department plays a leading role in counter-intelligence and national security investigations that uncover threats to our computer networks. Through the Department's National Security Division (NSD), we investigate, prevent, and prosecute where appropriate, the cyber activities of nation-states and terrorists that pose a threat to our national security. In addition, NSD exercises oversight authority over foreign intelligence collection efforts within the United States.

Enforcement

One key part of the nation's overall cybersecurity effort is the investigation and prosecution of cyber criminals—with the goal of incapacitating or deterring them before they can complete an attack on our networks, or punishing them and deterring similar future acts if there is a successful intrusion.

The Department has organized itself to ensure that we are in a position to aggressively investigate and prosecute cyber crime wherever it occurs. The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), together with a nationwide network of 230 Computer Hacking and Intellectual Property (CHIP) prosecutors in our United States Attorney's Offices (USAOs), take a leading role in promoting and leading our efforts to investigate and prosecute cyber offenses. These prosecutors, as well as other prosecutors 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 National Cyber Investigative Joint Task Force, 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.

Litigating components of the Department's National Security Division—the Counterespionage and Counterterrorism Sections—share the Criminal Division's and the USAOs' responsibility for safeguarding the country's information systems through enforcement of criminal laws. The Counterespionage Section prosecutes 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—leveraging the capabilities and expertise of CCIPS, CHIP prosecutors, the Anti-Terrorism Advisory Council, and Joint Terrorism Task Forces—would play a pivotal role in addressing any major cybersecurity attack by terrorists or associated groups or individuals.

Operational Successes

The relationships between the Department's prosecuting components and the federal investigative agencies, and the robust cooperation and information sharing that they support, have led to a number of enforcement successes—just a few of which I would like to highlight here.

Trade secrets and the Insider Threat. In March 2011, a former computer programmer at Goldman Sachs & Co. was sentenced in Manhattan federal court to 97 months in prison for stealing valuable, proprietary computer code of Goldman Sachs. A jury previously found the defendant guilty of theft of trade secrets and interstate transportation of stolen property.

In February 2011, a former trader at Société Générale was sentenced in Manhattan to 36 months in prison for theft of trade secrets and interstate transportation of stolen property. In November 2010, a jury convicted the trader of stealing proprietary computer code used in the company's high frequency trading business and of interstate transportation of the stolen code.

Also in February 2011, a federal jury in Louisiana convicted a former research scientist of stealing trade secrets from Dow Chemical Company and selling them to companies in the People's Republic of China. According to the evidence presented in court, the defendant came to the United States from China for graduate work. He began working for Dow in 1965 and retired in 1992. Dow is a leading producer of the elastomeric polymer, chlorinated polyethylene (CPE). Dow's CPE is used in a number of applications worldwide, such as automotive and industrial hoses, electrical cable jackets and vinyl siding. The evidence at trial established that the defendant conspired with at least four current and former employees of Dow's facilities to misappropriate those trade secrets, in part by accessing Dow's computers, in an effort to develop and market CPE process design packages to various Chinese companies. The defendant traveled extensively throughout China to market the stolen information, and evidence introduced at trial showed that he paid current and former Dow employees for Dow's CPE-related material and information. The defendant is awaiting sentencing.

Global hacking and identity theft case. In August 2008, the Department, working closely with the Secret Service, announced one of the largest hacking and identity theft cases ever prosecuted, in which charges were brought by the USAOs in the District of Massachusetts, the Southern District of California, and the Eastern District of New York against 11 members of an international hacking ring responsible for the theft and sale of more than 40 million credit and debit card numbers obtained from various retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave &

Buster's, and DSW. The various defendants—who were from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus—included one of the top traffickers in stolen account information in the world, Maksym Yastremski, and one of the world's top hackers, Albert Gonzalez. Gonzalez pleaded guilty and was sentenced to 20 years in prison. Yastremski was convicted on related charges in Turkey and was later sentenced to 30 years in prison.

Gonzalez and two unnamed hackers believed to be residing in Russia were also indicted for conspiring to hack into computer networks supporting major American retail and financial organizations and stealing data relating to more than 130 million credit and debit cards. Among the corporate victims were Heartland Payment Systems, 7-Eleven Inc., and Hannaford Brothers Co. Inc. Mr. Gonzalez pleaded guilty to the charges and received a sentence of over 20 years in prison to run concurrently with his other sentence.

Sophisticated ATM fraud hacking ring. In November 2009, the Department announced the indictment in the Northern District of Georgia of a sophisticated international hacking ring that executed a $9 million fraud scheme that involved five defendants from Estonia, one from Russia, and one from Moldova. The indictment charged various defendants with hacking into a computer network operated by the credit card processing company RBS WorldPay and using sophisticated techniques to compromise the data encryption used by RBS WorldPay to protect customer data on payroll debit cards. Once the defendants had compromised the encryption on the card processing system, the hacking ring allegedly provided a network of "cashers" with 44 counterfeit payroll debit cards. The cashers used these cards to withdraw over $9 million from more than 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada. Remarkably, the $9 million loss occurred within a span of less than 12 hours. The five Estonian defendants have been arrested and charged in Estonia. One of these defendants was extradited to the United States in August 2010. Through this investigation, the FBI uncovered a previously undetected hacking technique that compromised the bank's encryption system. This information was disseminated throughout the banking sector to prevent further losses.

International Online Tax Fraud Scheme. In January 2011, a Belarusian national residing in Massachusetts pled guilty to crimes stemming from his participation in an international online scheme to steal income tax refunds from U.S. taxpayers around the country. From 2006 through 2007, the defendant's co-conspirators lured victims by operating "phishing" websites that falsely claimed to be authorized by the IRS to offer lower-income taxpayers free online tax return preparation and electronic tax return filing services. After taxpayers uploaded their tax information, co-conspirators in Belarus collected the data and altered the returns to increase the refund amounts and to direct these refunds to be deposited into U.S. bank accounts controlled by the defendant. They then caused the fraudulently altered returns to be e-filed with the IRS. The conspiracy ultimately caused the U.S. Treasury and various state treasury departments to deposit more than $200,000 in stolen refunds into bank accounts controlled by the defendant.

Large-scale spam. In December 2010, a Russian citizen was charged with violating the CAN-SPAM Act. The indictment alleged that the defendant knowingly and materially falsified header information in billions of spam emails on behalf of individuals who were selling counterfeit Rolexes, non-FDA approved herbal remedies, and counterfeit prescription medications. In payment, the defendant received hundreds of thousands of dollars. The defendant is alleged to have initiated the sending of these messages by use of his botnet, dubbed the "Mega-D" botnet. This botnet compromised the security of tens of thousands of computers in the United States and around the world. The Mega-D botnet was capable of sending ten billion spam email messages a day, all with false header information.

Romanian Fraud Rings. In April 2010, Romanian police arrested 70 suspects who allegedly were involved in eBay scams and other cybercrimes since 2006. These arrests were the result of an international investigation dubbed Operation Valley of the Kings – a joint operation among the FBI, the Secret Service, and the Romanian Directorate for Investigating Organised Crime and Terrorism, involving hundreds of law enforcement agents in multiple cities and more than 100 search warrants. The arrested individuals allegedly used phishing attacks to get the login credentials of eBay account holders and then used the accounts to auction nonexistent goods. Police estimate that victims suffered approximately $1 million in losses after sending money for winning "auctions" but receiving no goods. Approximately 800 victims have been identified, and it is believed that the perpetrators operated in Austria, Canada, Denmark, France, Germany, Italy, New Zealand, Spain, Sweden, Switzerland, and the United States.

* * *

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. 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.

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

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