Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SENATE JUDICIARY COMMITTEE

SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

AT A HEARING ENTITLED

"CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY RIGHTS IN CYBERSPACE"

PRESENTED

NOVEMBER 17, 2009

Good afternoon, Chairman Cardin, Ranking Member Kyl, and Members of the Senate Judiciary Terrorism and Homeland Security Subcommittee. It is a pleasure to appear before you to testify about securing our nation's information infrastructure. 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. 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.

I. Cybersecurity Threats

As you know, information technology is embedded within and interconnects virtually all of the Nation's information and communications infrastructure, which we depend upon to conduct commercial, financial, personal, and governmental transactions. We face ongoing threats to the security of our information and information 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 disrupt services, including those provided by critical infrastructures.

As recognized in the Preface to the President's *Cyberspace Policy Review*, a 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cybersecurity,

> [t]he architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations.

Our reliance on our digital infrastructure requires that we take action to protect not only the information infrastructure itself, but also all of 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 tools to bear in the fight against cyber adversaries. The Department of Justice plays a key role in that fight.

II. 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 Homeland Security, and the Department of Defense – to support cybersecurity efforts and inform policy discussions, as we did during the President's Cyberspace Policy Review, which was completed in May 2009. We also work closely with the National Security Council to provide legal guidance related to the unique challenges posed by threats in cyberspace, on topics 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 most vigorously protect privacy and civil liberties while still achieving our goal of securing the Nation's information infrastructure. With respect to the EINSTEIN program, the Department has made public two opinions from the Office of Legal

Counsel regarding that program. I will not repeat that legal analysis here but I am prepared to address any questions that members of the Subcommittee may have in that regard.

In addition, the Department has responsibility for the enforcement of laws that help secure our data and computers and for the domestic collection of foreign intelligence information, including intelligence that supports cybersecurity efforts. Through the Department's Criminal Division, especially its Computer Crime and Intellectual Property Section (CCIPS) and the U.S. Attorneys' Offices (USAOs) across the country, in coordination with our law enforcement partners at the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS), among others, we have the authority to investigate and prosecute criminal cyber actors who threaten our nation's cybersecurity. And through the Department's National Security Division (NSD), we investigate, prosecute, and prevent 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 to protect the civil liberties and privacy rights of U.S. persons.

I would like to outline briefly some of these efforts – enforcement and collection – as well as our other cybersecurity legal and policy work and our role in the protection of civil liberties and privacy.

III. 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. A nationwide network of over 230 Computer Hacking and Intellectual Property (CHIP) prosecutors in our USAOs focuses on these crimes, coordinated through the Criminal Division's CCIPS. These prosecutors, as well as all prosecutors working cybercrime cases throughout the country, work closely with all of our law enforcement partners, including the FBI, the USSS, 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.

Litigating components of the Department's NSD -- the Counterespionage and the Counterterrorism Sections -- share the Criminal Division's 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 section 1030(a)(1) of 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.

A. 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.

- **Phish Phry.** Last month, 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. "Phishing" is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. 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 identify theft. This investigation, led by the FBI, required close coordination with the USSS, the Electronic Crimes Task Force, the USAO in the Central District of California, state and local law enforcement, and our Egyptian counterparts. In fact, Phish Phry represents the first joint cyber investigation between Egypt and the United States.

- **RBS WorldPay.** Just last week, as a result of unprecedented international law enforcement cooperation, four members of an alleged international hacking ring were indicted in Atlanta for their participation in a highly sophisticated and organized computer fraud attack. They face various charges related to allegedly hacking into a computer network operated by the Atlanta-based credit card processing company RBS WorldPay, which is part of the Royal Bank of Scotland. Sergei Tsurikov of Estonia, Viktor Pleshchuk of Russia, Oleg Covelin of Moldova, and a person known only as "Hacker 3" allegedly used sophisticated hacking techniques to compromise the data encryption that RBS WorldPay used to protect customer data on payroll debit cards, which enable employees to withdraw their regular salaries from an ATM. Once the encryption on the card processing system was compromised, the hacking ring allegedly raised the account limits on compromised accounts and then provided a network of "cashers" with 44 counterfeit payroll debit cards, which were used to withdraw more than $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. The $9 million loss occurred within a span of less than 12 hours. Four other individuals from Estonia were also charged in Atlanta with access device fraud for their involvement in the scheme. This investigation, led by the FBI,

required close coordination not only with other domestic law enforcement partners, including the USSS, the USAO in Atlanta, and various components of the Department's Criminal Division, including CCIPS and the Office of International Affairs, but also with numerous international partners, including the Estonian Central Criminal Police and the Estonian Office of the Prosecutor General, the Hong Kong Police Force, and the Netherlands Police Agency National Crime Squad High Tech Crime Unit and National Public Prosecutor's Office.

- **International hacking ring.** In September 2009, Albert Gonzalez, a hacker involved in one of the largest hacking and identity theft case ever prosecuted, pleaded guilty to 20 counts of conspiracy, computer fraud, wire fraud, access device fraud, and aggravated identity theft in the District of Massachusetts and the Eastern District of New York. Gonzalez was part of an international hacking ring responsible for the theft of more than 40 million credit and debit card numbers from various retailers, including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, Dave & Buster's, and DSW. In all, 11 ring members from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus were indicted in this case. Gonzalez remains under indictment in the District of New Jersey on charges related to a conspiracy to hack into computer networks supporting major U.S. retail and financial organizations, including Heartland Payment Systems and 7-Eleven, and steal credit and debit card numbers from those entities. Another defendant in this case, Maksym Yastremskiy, known online as "Maksik," was ultimately arrested for his carding activity in Turkey, and earlier this year, was sentenced by a Turkish court to 30 years in prison. Maksik is believed to be one of the top traffickers in stolen account information.

- **DarkMarket carding forum**. On October 16, 2008, the FBI announced the results of a two-year undercover operation, conducted in conjunction with CCIPS, targeting members of the online carding forum known as DarkMarket. At its peak, the DarkMarket website had over 2,500 registered members around the world. This operation, which required unprecedented international cooperation, involved law enforcement from countries ranging from Ukraine to Turkey to Romania to France. It resulted in approximately 60 arrests worldwide and prevented an estimated $70 million in economic loss.

- **"Hacker Havens."** A number of recent investigations begun in the U.S. have resulted in successful prosecutions in several foreign countries long considered to be so-called "hacker havens." As just one example, based on close cooperation between the Department, the FBI, and the Romanian National Police Cybercrime Divisions, prosecutors from Romania's Directorate for Investigating Organized Crime and Terrorism arrested 11 Romanian citizens on fraud and identity theft charges in November 2007. They were part of a criminal organization that specialized in "phishing" information from computer users, imprinting credit and debit card information onto counterfeit cards, and then using those cards to obtain cash from ATMs and Western Union locations. Romanian police officers executed 21 search warrants and seized computers, card reading and writing devices, blank cards, and

other equipment. More recently, between February 2008 and March 2009, over 40 defendants were charged in Romania – along with 12 in the United States – for their participation in a sophisticated hacking scheme involving the theft of corporate bank account information, and the use of that stolen information in a variety of fraudulent transactions.

- **Economic Espionage.** In June 2008, Xiaodong Sheldon Meng, a software engineer born in China, received the first sentence handed down by a federal court for a violation of the Economic Espionage Act for misappropriating intellectual property to benefit a foreign nation. He also was sentenced for violating the Arms Export Control Act and the International Traffic in Arms Regulations. Meng's conviction involved the theft of source code known as "Mantis 1.5.5" (simulator technology used for military training and other purposes) from his former employer, Quantum3D Inc., with the intent to benefit the People's Republic of China (PRC) Navy Research Center in Beijing.

It is important to understand that one of the key challenges that we face in pursuing cyber criminals is to accurately attribute the source of an intrusion. Often we cannot easily tell who is perpetrating these actions – a nation-state, a terrorist, or a criminal individual or group – but regardless of the actor, the effect is often the same. These kinds of cyber intrusions undermine the Nation's economic and national security, and the Department is committed to enforcing the laws designed to prohibit these incidents.

B. Capacity Building and Legal Tools

Beyond our own operational successes, the Department also engages in extensive capacity building through training programs, both domestic and international, that augment the U.S. Government's ability to investigate and prosecute cyber incidents. Every year, we train hundreds of domestic law enforcement agents on the legal tools we use in our enforcement efforts. These legal tools include substantive criminal laws that establish criminal conduct, such as the Computer Fraud and Abuse Act (18 U.S.C. § 1030), but also the laws that empower us to gather evidence to investigate such conduct, such as the Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.). The penalties for hacking crimes could be enhanced to better deter criminals, and a law requiring data breach reports to federal law enforcement would help us better investigate and prosecute large-scale security breaches. The Department stands ready to work with Congress to this end.

In addition, we engage extensively with our foreign law enforcement partners. Only by assisting foreign authorities can we expect them to reciprocate with vital evidence for our own investigations. As such, we often begin domestic investigations that lead to successful foreign prosecutions, as in the hacker haven cases I discussed above. And even purely domestic investigations often rely on evidence from overseas, such as where a U.S. hacker routes his communications through foreign computers before attacking a U.S. victim. CCIPS also is the United States Point of Contact in the G8 High-Tech Crime's 24/7 network, which consists of 55 member countries and is designed to connect international law enforcement partners with each other at any time to facilitate investigative cooperation.

Beyond this kind of assistance, we also train foreign law enforcement agencies each year on electronic evidence collection and international cooperation, and we provide technical and drafting assistance for countries developing laws criminalizing malicious cyber activity. To promote foreign legal development, we believe that the United States should continue to press other nations to accede to the Convention on Cybercrime (2001). Broader membership in the Convention will improve cooperation between law enforcement agencies by creating consistent substantive laws, and by improving procedural laws across the globe to facilitate the United States' ability to quickly and easily get foreign evidence required for a domestic investigation.

IV. Foreign Intelligence Collection and Oversight

The Department also supports the Intelligence Community's cybersecurity efforts through the work of NSD's Office of Intelligence. The Office of Intelligence plays a pivotal role in many facets of the Intelligence Community's efforts to protect the nation, including its burgeoning cybersecurity efforts. In particular, the Office of Intelligence represents the U.S. Government before the Foreign Intelligence Surveillance Court to obtain the authority for the FBI and other members of the Intelligence Community to collect foreign intelligence pursuant to the Foreign Intelligence Surveillance Act, as amended (50 U.S.C. § 1801, et seq.) (FISA). Because almost all activity conducted pursuant to FISA is classified, I am limited in what I can say in this hearing about the Department's cybersecurity activities under that statute. However, I would be happy to provide you with more information about such activities in an appropriate forum.

It is important for me to emphasize that in addition to providing support to the Intelligence Community's cybersecurity activities—as well as its other intelligence gathering responsibilities conducted domestically or involving U.S. persons abroad—the Department also has significant responsibilities for protecting civil liberties. While the Department has increased its efficiency in preparing and submitting FISA applications to the FISC, it also has enhanced its ability to ensure that these applications furnish all of the privacy protections provided by the FISA statute. Moreover, the Department has assumed increased responsibility for ensuring that the intelligence and counterintelligence activities of the FBI, as well as those of other intelligence agencies, adhere to the Constitution and applicable laws of the United States. Through activities such as the review and approval of guidelines as provided by Executive Order 12333 governing Intelligence Community activities, the Department plays a central role in safeguarding vital civil liberties as we help protect the Nation.

V. Other Cybersecurity Efforts

Finally, the Department plays a key role in the policy development process and the implementation of technical cybersecurity measures. The Department's Criminal Division, NSD, and Chief Information Officer's Office, have been heavily involved in interagency policy development on issues related to incident response, information sharing, technical architecture, coordinating cyber operations, international engagement, and public awareness.

The Department's Chief Information Officer (CIO) has also strengthened the Department's network defenses by reducing the number of Internet connections to consolidate traffic, providing in-depth monitoring of those connections and supporting security upgrades to gateway services. In addition, the Department CIO has recently invested in an enterprise tool that will provide real time situational awareness of network operations, monitor secure configuration controls and streamline patch management. The Department's Justice Security Operations Center (JSOC) analyzes EINSTEIN I data to support its mission of defending Department computer networks. While JSOC possesses more robust network traffic tools, the EINSTEIN I appliance provides an efficient mechanism to query network traffic flows in support of computer security incident response.

In addition to our policy work, the Department also plays a unique role in providing legal guidance on issues related to cybersecurity. Working in coordination with Offices of General Counsel throughout the U.S. Government, we have analyzed the EINSTEIN program, with which you are familiar, and taken steps to ensure that our cybersecurity efforts not only rest on sound legal footing but also vigorously protect civil liberties and privacy.

VI. **Existing Legal Authorities and Civil Liberties Protections**

One of the Department's responsibilities is to ensure that it is using existing legal authorities to the fullest extent possible, and to continually review those authorities to make sure that they are effective in addressing today's challenges. The law applicable to cyber-security activities is very complex and difficult to summarize succinctly. That domestic and international legal regime necessarily defines and limits available policy options, and impacts the relationship between the government and the private sector on cyber issues. As set forth in the Administration's *Cyberspace Policy Review*:

> Law applicable to information and communications networks is a complex patchwork of Constitutional, domestic, foreign, and international laws that shapes viable policy options. In the United States, this patchwork exists because, throughout the evolution of the information and communications infrastructure, the Federal government enacted laws and policies to govern aspects of what were very diverse industries and technologies.
>
> As traditional telecommunications and Internet-type networks continue to converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity, law and policy should continue to seek an integrated approach that combines the benefits of flexibility and diversity of applications and services with the protection of civil liberties, privacy rights, public safety, and national and economic security interests . . . . Policy decisions will necessarily be shaped and bounded by the legal framework in which they are made, and policy consideration may help identify gaps and challenges in current laws and inform necessary developments in the law. That process may prompt proposals for a new legislative framework to rationalize the patchwork of overlapping laws that apply to information, telecommunications, networks, and technologies, or the application of new interpretations of existing laws in ways to meet technological evolution and policy goals, consistent with U.S. Constitutional principles. However, pursuing either

course risks outcomes that may make certain activities conducted by the Federal government to protect information and communications infrastructure more difficult.

The Department looks forward to continuing to work with Congress to better ensure that our laws address properly the threats and challenges that all of us – including the government, the private sector, and the public – face today and provide for appropriately robust law enforcement, intelligence, and other cyber-related authorities, consistent with civil liberties and privacy protections. As noted above, any changes we make must be well-considered to reduce the likelihood that they will have unintended consequences that adversely impact law enforcement or intelligence activities or privacy rights.

VII. Conclusion

I would like to thank the Subcommittee for the opportunity to share with you, and the American people, the high priority the Department places on cybersecurity and the work we do to protect the Nation's information and communications infrastructure through cyberspace policy development, law enforcement, and intelligence collection. We recognize that each of the federal components testifying here today plays a distinct and vital role in cybersecurity, and we look forward to continuing to work with them and all of our partners throughout the government, in the private sector, and across the globe, to achieve our common goal of assuring a trusted and resilient information and communications infrastructure.

This concludes my remarks. I would be pleased to answer questions from you and other members of the Subcommittee.