Statement for the Record

Cybersecurity: Preparing for and Responding to the Enduring Threat

Acting Deputy Secretary Rand Beers
U.S. Department of Homeland Security

Before the
Senate Appropriations Committee

June 12, 2013

INTRODUCTION

Cyberspace is woven into the fabric of our daily lives. According to recent estimates, globally interconnected communications and information networks that operate in this space encompass more than two billion people with at least 12 billion computers and devices, including global positioning systems, mobile phones, satellites, data routers, ordinary desktop computers, and industrial control computers that run power plants, water systems, and more.

While this increased connectivity has led to significant transformations and advances across our country – and around the world – it also has increased the importance and complexity of our shared risk and requires a collaborative approach within government and between governments and the private sector. Our daily activities, economic vitality, and national security depend on the Nation's ability to secure cyberspace. A vast array of interdependent information technology (IT) networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks. The word "cybersecurity" itself encompasses prevention, protection and resilience against a broad range of malicious activity from a variety of actors perpetrating denial of service attacks, targeting our financial system to steal millions of dollars, accessing valuable trade secrets, and intruding into government networks and systems that control our critical infrastructure.

Cyber attacks and intrusions can have very real consequences in the physical world. The Department of Homeland Security (DHS) is the lead Federal civilian department responsible for coordinating the national protection, prevention, mitigation, and recovery from cyber incidents and works regularly with business owners and operators to take steps to strengthen their facilities and communities. The Department's National Cybersecurity and Communications Integration Center (NCCIC) works daily to enhance situational awareness among stakeholders, including those at the state and local level, as well as industrial control system owners and operators, by providing critical cyber threat, vulnerability, and mitigation data to a number of organizations including through Information Sharing and Analysis Centers, which are cybersecurity resources for critical infrastructure sectors. Last year DHS notified potential targets of a campaign of cyber intrusions that focused on natural gas and pipeline companies that was highly targeted, tightly focused and well crafted. With the assistance of our interagency partners, we responded to this campaign with a comprehensive effort that included outreach, technical assistance, and mitigation.

The U.S. Government has worked closely with the private sector during the recent series of denial-of-service incidents against the financial sector. Together with our interagency partners, we have provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities. This includes identifying and releasing hundreds of thousands of distributed denial of service-related IP addresses and supporting information in order to help financial institutions and their IT security service providers improve their defenses. In addition to sharing with these private sector entities, DHS working with the Department of State (DOS) has provided this threat information to more than 120 international partners, many of whom have contributed to our mitigation efforts. These developments reinforce the need for greater

information sharing and collaboration among government, industry, and individuals to reduce the ability for malicious actors to establish and maintain capabilities to carry out such efforts.

In addition to these attacks and intrusions, we also face a range of traditional crimes now perpetrated through cyber networks. These include child pornography and exploitation, as well as banking and financial fraud, all of which pose severe economic and human consequences. For example, in March 2012, the U.S. Secret Service (USSS) worked with U.S. Immigration and Customs Enforcement (ICE) to arrest nearly 20 individuals in its "Operation Open Market," which seeks to combat transnational organized crime, including the buying and selling of stolen personal and financial information through online forums.

Additionally, in late May 2013, the Secret Service, in close coordination with U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the Global Illicit Financial Team, arrested five individuals and seized bank accounts containing approximately $20 million located in eight countries. The investigation of Liberty Reserve, a transnational online payment processor and money transfer system, led to the seizure of an online domain owned and operated by the company. It is alleged that Liberty Reserve is used by criminal elements worldwide to launder money and distribute illegal proceeds globally. Liberty Reserve had approximately one million users worldwide with more than 200,000 users in the United States. It is estimated that Liberty Reserve processed more than 12 million financial transactions annually with a combined value of more than $1.4 billion. Overall, Liberty Reserve processed an estimated 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds. The United States Attorney's Office for the Southern District of New York is prosecuting this case.

As Americans become more reliant on modern technology, we also become more vulnerable to cyber exploits such as corporate security breaches, social media fraud, and spear phishing, which targets employees through emails that appear to be from people they know, allowing cyber criminals to steal personal and business information.

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require engagement from government, the private sector, law enforcement, and members of the public. The success of our efforts to reduce cybersecurity risks depends on effective identification of cyber threats and vulnerabilities, analysis, and enhanced information sharing between departments and agencies from all levels of government, the private sector, international entities, and the American public.

DHS MISSION IN PROTECTING GOVERNMENT NETWORKS AND CRITICAL INFRASTRUCTURE

DHS is committed to ensuring cyberspace is supported by a secure and resilient infrastructure that enables open communication, innovation, and prosperity while protecting privacy, confidentiality, and civil rights and civil liberties by design. The Department is achieving its cybersecurity mission by helping to create a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation.

DHS has operational responsibilities for securing unclassified federal civilian government networks and working with owners and operators of critical infrastructure to secure their networks through cyber threat analysis, risk assessment, mitigation, and incident response capabilities. The Department is also responsible for coordinating the Federal Government response to significant cyber or physical incidents affecting critical infrastructure consistent with Presidential Policy Directive (PPD) 21. In addition, the Department combats cyber crime by leveraging the skills and resources of the USSS and ICE and working in cooperation with partner organizations to investigate cyber criminals. In addition, pursuant to the President's recent Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, we are working with our partners to strengthen the security and resilience of critical infrastructure through an updated and overarching national framework that acknowledges the increased role of cybersecurity in securing physical assets.

RESPONSE TO CYBER EVENTS

The NCCIC is a key component of DHS's ability to work with government, industry, and international partners to protect critical cyber and communications systems. To create shared situational awareness, the NCCIC integrates internal analysis and data, intelligence community and law enforcement reporting, and data shared by private sector and international partners into a comprehensive series of actionable information products, including joint products with the Federal Bureau of Investigation (FBI). The NCCIC works closely with those Federal agencies most responsible for helping to enhance the cybersecurity of critical infrastructures, including the Departments of Treasury and Energy.

In addition to federal partners, the NCCIC also actively engages with the appropriate private sector entities; information sharing and analysis centers; state, local, tribal, and territorial (SLTT) governments, including the Multi-State Information Sharing and Analysis Center (MS-ISAC); and international partners. As integral parts of the cybersecurity and communications community, these groups work together to protect the portions of critical information technology that they interact with, operate, manage, or own. The NCCIC leverages the collective capabilities of its partners to provide joint incident response to assist with forensic investigations, malware analysis, review network data, and security posture assessment.

To further increase awareness of both cyber threat and resources available, the NCCIC and the United States Computer Emergency Readiness Team (US-CERT) have conducted approximately 50 threat briefings thus far in Fiscal Year (FY) 2013 as a part of our outreach effort to our Federal, SLTT, and private sector partners. Since 2009, the NCCIC has responded to nearly half a million incident reports and released more than 26,000 actionable cybersecurity alerts to the Department's public and private sector partners. An integral player within the NCCIC, the US-CERT also provides response support and defense against cyber-attacks for Federal civilian agency networks as well as private sector partners upon request. US-CERT collaborates and shares information with state and local government, industry, and international partners, consistent with rigorous privacy, confidentiality, and civil liberties guidelines, to address cyber threats and develop effective security responses. In 2012, US-CERT processed approximately

190,000 cyber incidents involving Federal agencies, critical infrastructure, and the Department's industry partners – a 68 percent increase from 2011. In addition, US-CERT issued over 20,411 actionable cyber-alerts over the past three years that were used by private sector and government agencies to protect their systems.

Similar growth has been seen for the Department's Industrial Control Systems Computer Emergency Response Team (ICS-CERT) and National Coordinating Center for Telecommunications (NCC), whose outreach has resulted in providing access to cyber threat information to more than 980 and 300 entities, respectively. ICS-CERT also responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US-CERT to assist with significant private sector cyber incidents. This rapid increase in production for ICS-CERT, including the dissemination of more than 800 products over the past three years, yielded them the award of Best Security Team by SC Magazine at the 2013 RSA Security Conference.

The effectiveness of DHS's cyber protection, response, mitigation and recovery relies heavily on sharing information with the private sector. In 2011, DHS launched the Cyber Information Sharing and Collaboration Program (CISCP), which is specifically designed to elevate the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. The Department is constantly enhancing the CISCP. In an effort to ensure the program continues to evolve with the needs of industry, DHS has conducted numerous feedback sessions, monthly collaboration conference calls, and three face-to-face technical exchanges. It is also working to automate the program so that it can share information in real-time.

In addition to the CISCP, DHS, in close collaboration with interagency and private sector partners, is continuing to expand the Enhanced Cybersecurity Services (ECS) program, which establishes a voluntary information sharing program that assists critical infrastructure owners and operators to improve protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the U.S. Government to gain access to a broad range of cyber threat information. ECS consists of the operational processes and security oversight required to share sensitive and classified cyber threat information with qualified Commercial Service Providers (CSP). The ECS program develops threat "indicators" with this information and provides CSPs with those indications of active, malicious cybersecurity activity to better protect their critical-infrastructure customers.

In FY 2013, DHS has already shared more than 200,000 indicators via the ECS program and other Joint Indicator Bulletin products with partners for computer network defense. CSPs may use these threat indicators to provide approved cybersecurity services to critical infrastructure entities. ECS augments, but does not replace, entities' existing cybersecurity capabilities. The program was also built with privacy and civil liberties protections in mind. Consistent with their commercial agreements with the protected entities, CSPs are not required to share with the Government, but may voluntarily do so. The incident information is anonymized, unless the protected entity consents to having its identity provided to DHS.

COMBATING CYBER CRIME

DHS employs more law enforcement agents than any other Department in the Federal Government and has personnel stationed in every state and in more than 75 countries around the world. Since 2009, DHS has prevented $10 billion in potential losses through cyber crime investigations and arrested more than 5,000 individuals for their participation in cyber crime activities.

The Department leverages the 31 USSS Electronic Crimes Task Forces (ECTF), which combine the resources of academia, the private sector, and local, state and Federal law enforcement agencies to combat computer-based threats to our financial payment systems and critical infrastructure. A recently executed partnership between ICE Homeland Security Investigations and USSS demonstrates the Department's commitment to leveraging capability and finding efficiencies. Both organizations will expand participation in the existing ECTFs. In addition to strengthening each agency's cyber investigative capabilities, this partnership will produce benefits with respect to the procurement of computer forensic hardware, software licensing, and training that each agency requires. The Department is also a partner in the National Cyber Investigative Joint Task Force, which serves as a collaborative entity that fosters information sharing across the interagency.

In FY 2012, the Secret Service arrested 1,378 individuals for cyber-crime violations while maintaining a 99.6% conviction rate; these criminals were responsible for over $335 million in fraud losses and could have potentially caused over $1.2 billion in fraud loss based on financial account information in their possession at the time of their arrest. As part of its protective duties, the Secret Service has developed a Critical Systems Protection Program, which assesses and mitigates the risks to critical infrastructure that could impact Secret Service protectees or National Special Security Events (NSSEs). This program applies risk management practices developed by the National Institute of Standards and Technology to help critical infrastructure owners and operators secure their systems from cyber threats. From October 2009 to May 2013 this program has conducted over 560 advances and secured 8 NSSEs.

In the course of investigating cyber crimes over the last 30 years, the Secret Service has developed a number of cybersecurity capabilities to support its mission. The backbone of the ECTFs is its Electronic Crimes Special Agent Program (ECSAP), which is comprised of nearly 1,400 Secret Service special agents who have received at least one of three levels of computer crimes-related training. These agents are deployed in more than 98 Secret Service offices throughout the world and have received training in forensic identification, preservation and retrieval of electronically stored evidence. ECSAP-trained agents are computer investigative specialists, qualified to conduct examinations on all types of electronic evidence. These special agents are equipped to investigate the continually evolving arena of electronic and cyber crimes and have proven invaluable in the successful prosecution of criminal groups involved in computer fraud, bank fraud, identity theft, access device fraud and various other electronic and cyber crimes targeting our financial institutions and private sector. USSS also supports state and local law enforcement, in addition to other Federal agencies, by making these capabilities

available to support their operations.[1] They include computer forensics specialists, mobile wireless investigation teams, and advanced research support.

To expand its collaborative efforts, the Secret Service provides its ECSAP training to investigators at the ICE Computer Crimes Center as well as via the National Computer Forensics Institute (NCFI), which is a result of a partnership between the National Protection and Programs Directorate, the Secret Service, the State of Alabama, the City of Hoover, Shelby County, the Alabama District Attorney's Association, and the Alabama Securities Commission, established to provide computer forensic training and tools to state and local law enforcement officers, prosecutors, and judges. Investigators are trained to respond to network intrusion incidents and conduct electronic and cyber crimes investigations. This training also has the benefit of providing state and local law enforcement with the skills and tools to combat a myriad of crimes in their community. Further, the NCFI has supported training for DHS Fusion Centers and the FBI's National Domestic Communications Assistance Center. Responding to the growth of cyber crimes and the level of sophistication these criminals employ requires training, resources and greater collaboration among law enforcement and its public and private sector partners. Since opening in May 2008, NCFI has trained more than 2,050 state and local officials, including more than 1,360 police investigators, 525 prosecutors and 165 judges from all 50 states and three U.S. territories.

In addition to these activities, ICE HSI's Cyber Crimes Center (C3) delivers computer-based technical services to support domestic and international investigations into cross-border crime. C3 is made up of the Cyber Crimes Unit, the Child Exploitation Investigations Unit and the Computer Forensics Unit. This state-of-the-art center offers cyber crime support and training to federal, state, local and international law enforcement agencies. C3 also operates a fully equipped computer forensics laboratory, which specializes in digital evidence recovery, and offers training in computer investigative and forensic skills

COOPERATION ACROSS THE FEDERAL GOVERNMENT

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, national defense, and intelligence authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. DHS, the Department of Justice (DOJ), and the Department of Defense (DOD) each play a key

[1] Included are the following:

- Computer forensics specialists, which in FY 2012 conducted over 7,000 digital forensics exams, totaling over 1,100 terabytes of data;
- Cell Phone Forensics Facility at University of Tulsa, which since opening in 2008 has supported 6,135 exams, and 305 advanced exams at the University of Tulsa;
- 22 Mobile Wireless Investigations Teams, which in FY 2012 conducted nearly 1,140 investigations, supporting primarily state and local law enforcement with this advanced capability and directly contributing to solving homicide cases and locating missing persons;
- Advanced research support at Carnegie Mellon and development of advanced tools for use by law enforcement partners; and
- Support of landmark research studies, like the Insider Threat Report, Verizon Data Breach Investigations Report, and the Trust wave Global Security Report, which are an effective way to share law enforcement information, while protecting victim privacy, to develop national understanding of cyber risks.

role in responding to cybersecurity incidents that pose a risk to the United States. To achieve a whole of government response to specific cyber incidents, DHS, DOJ, and DOD synchronize their operations. The leaders of DHS, DOJ, and DOD have held a series of meetings to clarify the lanes in the road in cyber jurisdiction. The group agreed that DHS' primary role is to protect critical infrastructure and networks, coordinate mitigation and recovery, disseminate threat information across various sectors and investigate cybercrimes under DHS's jurisdiction. DOJ is the lead for investigation, enforcement, and prosecution of those responsible for cyber intrusions affecting the United States. As part of DOJ, the FBI conducts domestic national security operations; investigates, attributes, and disrupts cybercrimes; and collects, analyzes, and disseminates domestic cyber intelligence. DOD's role is to defend the nation, gather intelligence on foreign cyber threats, and to protect national security systems. DHS supports our partners in many ways. For example, the United States Coast Guard as an Armed Force has partnered with U.S. Cyber Command and U.S. Strategic Command to prepare for military cyberspace operations as directed. In coordination with DOS, DHS also works with international partners in strategic and operational engagements.

While each agency operates within the parameters of its authorities, the U.S. Government's response to cyber incidents of consequence is coordinated among these three agencies such that "a call to one is a call to all." Synchronization among DHS, DOJ, and DOD not only ensures that whole of government capabilities are brought to bear against cyber threats, but also improves government's ability to share timely and actionable cybersecurity information among a variety of partners, including the private sector.

PRESIDENTIAL POLICY DIRECTIVE 21 AND CYBER EXECUTIVE ORDER 13636

America's national security and economic prosperity are increasingly dependent upon the cybersecurity of critical infrastructure. With today's physical and cyber infrastructure growing more inextricably linked, critical infrastructure and emergency response functions are inseparable from the information technology systems that support them. The Federal Government's role in this effort is to share information and to encourage enhanced security and resilience, while also identifying gaps not filled by the marketplace. As mentioned previously, the enhanced information sharing programs supported by Executive Order 13636 and PPD-21 help secure critical infrastructure and increase its resilience against cyber and physical attacks, as well as natural disasters and terrorist attacks.

To complement PPD-21, EO 13636 promotes more efficient sharing of cyber threat information with the private sector and directs the establishment of a cybersecurity framework to identify and implement better security practices among critical infrastructure sectors. Through partnerships between the Government and private sector, the critical infrastructure cyber systems upon which much of our economic well-being, national security, and daily lives depend are being better protected. PPD-21 and EO 13636 reinforce holistic thinking and action in the realms of security and risk management and the issuance of these important documents allows us to build upon and enhance our existing partnership model with our key private sector and SLTT partners. Implementation of EO 13636 and PPD-21 will also drive action toward system and network security and resilience. The Department is well positioned to make advances in the space defined by the cyber-physical security nexus that PPD-21 and EO 13636 address.

BUDGET PRIORITIES

The FY 2014 Budget supports initiatives to secure our Nation's information and financial systems and to defend against cyber threats to private-sector and Federal systems, the Nation's critical infrastructure, and the U.S. economy. Taken together, the Administration's initiatives strengthen the security and resilience of critical infrastructure against evolving threats through an updated and overarching national framework that acknowledges the linkage between cybersecurity and securing physical assets.

Included in the FY 2014 Budget are enhancements to the National Cybersecurity Protection System (NCPS) to prevent and detect intrusions on government computer systems and to the National Cybersecurity and Communications Integration Center to protect against and respond to cybersecurity threats. The Budget also leverages the new operational partnership between ICE and USSS through the established network of USSS ECTFs to safeguard the Nation's financial payment systems, combat cybercrimes, target transnational child exploitation including large-scale producers and distributors of child pornography, and prevent attacks against U.S. critical infrastructure.

- *Federal Network Security:* $200 million is included for Federal Network Security, which manages activities designed to enable Federal agencies to secure their IT networks. The Budget provides funding to further reduce risk in the Federal cyber domain by enabling continuous monitoring and diagnostics of networks in support of mitigation activities designed to strengthen the operational security posture of Federal civilian networks. DHS will directly support Federal civilian departments and agencies in developing capabilities to improve their cybersecurity posture and to better thwart advanced, persistent cyber threats that are emerging in a dynamic threat environment.

- *NCPS:* $406 million is included for Network Security Deployment, which manages NCPS, operationally known as EINSTEIN. NCPS is an integrated intrusion detection, analytics, information-sharing, and intrusion-prevention system that supports DHS responsibilities to defend Federal civilian networks.

- *US-CERT:* $102 million is included for operations of US-CERT, which leads and coordinates efforts to improve the Nation's cybersecurity posture, promotes cyber information sharing, and manages cyber risks to the Nation. US-CERT encompasses the activities that provide immediate customer support and incident response, including 24-hour support in the National Cybersecurity and Communications Integration Center. As more Federal network traffic is covered by NCPS, additional US-CERT analysts are required to ensure cyber threats are detected and the Federal response is effective.

- *SLTT Engagement:* In FY 2014, DHS will expand its support to the MS-ISAC to assist in providing coverage for all 50 states and 6 U.S. territories in its managed security services program. MS-ISAC is a central entity through which SLTT governments can strengthen their security posture through network defense services and receive early

warnings of cyber threats. In addition, the MS-ISAC shares cybersecurity incident information, trends, and other analysis for security planning.

- *Cybersecurity Research and Development:* The FY 2014 Budget includes $70 million for the Science and Technology Directorate's research and development focused on strengthening the Nation's cybersecurity capabilities.

- *Cyber Investigations:* The FY 2014 Budget continues to support ICE and USSS to strategically investigate domestic and international criminal activities, including computer fraud, network intrusions, financial crimes, access device fraud, bank fraud, identity crimes and telecommunications fraud, benefits fraud, arms and strategic technology, money laundering, counterfeit pharmaceuticals, child pornography, and human trafficking occurring on or through the Internet. The Budget continues to enable these DHS law enforcement agencies to provide computer forensics support and training for law enforcement partners to enable them to effectively investigate cyber crime and conduct other highly-technical investigations. ICE projects an FY 2014 expenditure of $13.8 million for the Cyber Crimes Center supporting investigations to identify, disrupt, and dismantle domestic and transnational criminal organizations engaged in crimes facilitated by use of computers and cyberspace. In addition, ICE expects to spend $96.5 million on investigations of cyber crime/child exploitation. Other investigations of illicit trade, travel and finance all make use of cyber investigative techniques including computer forensic analysis. The Secret Service's ECTFs will also continue to focus on the prevention of cyber attacks against U.S. financial payment systems and critical infrastructure through aggressive investigation and information sharing.

- *Cyber Protection*: The FY 2014 budget includes $13.5 million to enhance the Secret Service's ability to secure protective venues, National Special Security Events and associated Critical Infrastructure/Key Resources from cyber attacks.

Cyber Legislative Priorities

It is important to note that the Executive Order directs Federal agencies to work within current authorities and increase voluntary cooperation with the private sector to provide better protection for computer systems critical to our national and economic security. It does not grant new regulatory authority or establish additional incentives for participation in a voluntary program. We continue to believe that a suite of legislation is necessary to implement the full range of steps needed to build a strong public-private partnership, and we will continue to work with Congress to achieve this.

To help us achieve our mission, we have created a number of competitive scholarship, fellowship, and internship programs to attract top talent. We are growing our world-class cybersecurity workforce by creating and implementing standards of performance, building and leveraging a cybersecurity talent pipeline with secondary and post-secondary institutions nationwide, and institutionalizing an effective, ongoing capability for strategic management of the Department's cybersecurity workforce. Congress can support this effort by pursuing legislation that provides DHS with the hiring and pay flexibilities we need to secure Federal

civilian networks, protect critical infrastructure, respond to cyber threats, and combat cybercrime.

CONCLUSION

The American people expect us to secure the country from the growing danger of cyber threats and ensure the nation's critical infrastructure is protected. The threats to our cybersecurity are real, they are serious, and they are urgent. I appreciate this Committee's guidance and support as, together, we work to keep our Nation safe.