Written testimony of DHS Deputy Secretary Jane Holl Lute for a House Committee on Homeland Security hearing titled “DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure”

Release Date:
March 13, 2013

311 Cannon House Office Building

Chairman McCaul, Ranking Member Thompson, and Members of the Committee:

I am pleased to join you today, and I thank the Committee for your strong support for the Department of Homeland Security (DHS) over the past four years and, indeed, since the Department’s founding ten years ago.

I can think of no more urgent and important topic in today’s interconnected world than cybersecurity, and I appreciate the opportunity to explain the Department’s mission in this space and how we continue to improve cybersecurity for the American people as well as work to safeguard the nation’s critical infrastructure and protect the Federal Government’s networks.

Current Threat Landscape

Cyberspace is woven into the fabric of our daily lives. According to recent estimates, this global network of networks encompasses 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. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent 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 protection against a broad range of malicious activity, from denial of service attacks, to theft of valuable trade secrets, to intrusions against government networks and systems that control our critical infrastructure.

The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Cyber crime has also increased significantly over the last decade. Sensitive information

is routinely stolen from both government and private sector networks, undermining the integrity of the data contained within these systems. We currently see malicious cyber activity from foreign nations engaged in espionage and information warfare, terrorists, organized crime, and insiders. Their methods range from distributed denial of service (DDoS) attacks and social engineering to viruses and other malware introduced through thumb drives, supply chain exploitation, and leveraging trusted insiders' access.

We have seen motivations for attacks vary from espionage by foreign intelligence services to criminals seeking financial gain and hackers who may seek bragging rights in the hacker community. Industrial control systems are also targeted by a variety of malicious actors who are usually intent on damaging equipment and facilities or stealing data. Foreign actors are also targeting intellectual property with the goal of stealing trade secrets or other sensitive corporate data from U.S. companies in order to gain an unfair competitive advantage in the global market.

Cyber attacks and intrusions can have very real consequences in the physical world. Last year, DHS identified a campaign of cyber intrusions targeting natural gas and pipeline companies that was highly targeted, tightly focused and well crafted. Stolen information could provide an attacker with sensitive knowledge about industrial control systems, including information that could allow for unauthorized operation of the systems. As the President has said, we know that our adversaries are seeking to sabotage our power grid, our financial institutions, and our air traffic control systems. These intrusions and attacks are coming all the time and they are coming from different sources and take different forms, all the while increasing in seriousness and sophistication.

The U.S. Government has worked closely with the private sector during the recent series of denial-of-service incidents. We have provided classified cyber threat briefings and technical assistance to help banks improve their defensive capabilities and we have increased sharing and coordination among the various government elements in this area. These developments reinforce the need for 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 sophisticated attacks and intrusions, we also face a range of traditional crimes that are 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. 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 colleagues within their own organizations, allowing cyber criminals to steal information.

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of our entire society—from government and law enforcement to the private sector and, most importantly, members of the public. The key question, then, is how do we address this problem? This is not an easy question because cybersecurity requires a layered approach. 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.

Roles, Responsibilities, Activities

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.

Securing Federal Civilian Government Networks

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. We also are responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the government.

DHS directly supports federal civilian departments and agencies in developing capabilities that will improve their cybersecurity posture in accordance with the Federal Information Security Management Act (FISMA). To protect Federal civilian agency networks, our National Protection and Programs Directorate (NPPD) is deploying technology to detect and block intrusions through the National Cybersecurity Protection System and its EINSTEIN protective capabilities, while providing guidance on what agencies need to do to protect themselves and measuring implementation of those efforts.

NPPD is also developing a Continuous Monitoring as a Service capability, which will result in an array of sensors that feed data about an agency's cybersecurity risk and present those risks in an automated and continuously-updated dashboard visible to technical workers and managers to enhance agencies' ability to see and counteract day-to-day cyber threats. This capability will support compliance with Administration policy, be consistent with guidelines set forth by the National Institute of Standards and Technology (NIST), and enable Federal agencies to move from compliance-driven risk management to data-driven risk management. These activities will provide organizations with information necessary to support risk response decisions, security status information, and ongoing insight into effectiveness of security controls.

Protecting Critical Infrastructure

Critical infrastructure is the backbone of our country's national and economic security. It includes power plants, chemical facilities, communications networks, bridges, highways, and stadiums, as well as the federal buildings where millions of Americans work and visit each day. DHS coordinates 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 also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners.

Protecting critical infrastructure against growing and evolving cyber threats requires a layered approach. DHS actively collaborates with public and private sector partners every day to improve the security and resilience of critical infrastructure while responding to and mitigating the impacts of attempted disruptions to the nation's critical cyber and communications networks and to reduce adverse impacts on critical network systems.

DHS enhances 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, including through Information Sharing and Analysis Centers, which are cybersecurity resources for critical infrastructure sectors. DHS is also home to the National Cybersecurity & Communications Integration Center (NCCIC), a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

Responding to Cyber Threats

DHS is responsible for coordinating the Federal Government response to significant cyber or physical incidents affecting critical infrastructure. Since 2009, the NCCIC has responded to nearly half a million incident reports and released more than 26,000 actionable cybersecurity alerts to our public and private sector partners. The DHS Office of Intelligence and Analysis is a key partner in NCCIC activities, providing tailored all-source cyber threat intelligence and warning to NCCIC components and public and private critical infrastructure stakeholders to prioritize risk analysis and mitigation.

An integral player within the NCCIC, the U.S. Computer Emergency Readiness Team (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 our industry partners. This represents a 68 percent increase from 2011. In addition, US CERT issued over 7,455 actionable cyber-alerts in 2012 that were used by private sector and government agencies to protect their systems, and had over 6,400 partners subscribe to the US CERT portal to engage in information sharing and receive cyber threat warning information.

The Department's Industrial Control Systems Cyber Emergency Response Team (ICS CERT) also responded to 177 incidents last year while completing 89 site assistance visits and deploying 15 teams with US-CERT to respond to significant private sector cyber incidents. DHS also empowers owners and operators through a cyber self-evaluation tool, which was used by over 1,000 companies last year, as well as in-person and on-line training sessions.

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military 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 role in responding to cybersecurity incidents that pose a risk to the United States. In addition to the aforementioned responsibilities of our Department, DOJ is the lead Federal department responsible for the investigation, attribution, disruption, and prosecution of domestic cybersecurity incidents while DOD is responsible for securing national security and military systems as well as gathering foreign cyber threat information and defending the nation from attacks in cyberspace. 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 conduct military cyberspace operations.

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.

Combating Cybercrime

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. To combat cyber crime, DHS relies upon the skills and resources of the USSS and ICE and works in cooperation with partner organizations to investigate cyber criminals. 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.

We work with a variety of international partners to combat cybercrime. For example, through the U.S.-EU Working Group on Cybersecurity and Cybercrime, which was established in 2010, we develop collaborative approaches to a wide range of cybersecurity and cybercrime issues. In 2011, DHS participated in the Cyber Atlantic tabletop exercise, a U.S.–EU effort to enhance international collaboration of incident management and response, and in 2012, DHS and the EU signed a joint statement

that advances transatlantic efforts to enhance online safety for children. ICE also works with international partners to seize and destroy counterfeit goods and disrupt websites that sell these goods. Since 2010, ICE and its partners have seized over 2,000 domain names associated with businesses selling counterfeit goods over the Internet. To further these efforts, the Administration issued its Strategy on Mitigating the Theft of U.S. Trade Secrets last month. DHS will act vigorously to support the Strategy's efforts to combat the theft of U.S. trade secrets – especially in cases where trade secrets are targeted through illicit cyber activity by criminal hackers.

In addition, the National Computer Forensic Institute has trained more than 1,000 state and local law enforcement officers since 2009 to conduct network intrusion and electronic crimes investigations and forensic functions. Several hundred prosecutors and judges as well as representatives from the private sector have also received training on the impact of network intrusion incident response, electronic crimes investigations, and computer forensics examinations.

Building Partnerships

DHS serves as the focal point for the Government's cybersecurity outreach and awareness efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the private or financial information of individuals is better protected. For example, the Multi-State Information Sharing and Analysis Center (MS-ISAC) opened its Cyber Security Operations Center in November 2010, which has enhanced NCCIC situational awareness at the state and local government level and allows the Federal Government to quickly and efficiently provide critical cyber threat, risk, vulnerability, and mitigation data to state and local governments. MS-ISAC has since grown to include all 50 states, three U.S. territories, the District of Columbia, and more than 200 local governments.

The Department also has established close working relationships with industry through partnerships like the Protected Critical Infrastructure Information (PCII) Program, which enhances voluntary information sharing between infrastructure owners and operators and the government. The Cyber Information Sharing and Collaboration Program established a systematic approach to cyber threat information sharing and collaboration between critical infrastructure owners and operators across the various sectors. And, in 2010, we launched a national campaign called *Stop.Think.Connect* to spread public awareness about how to keep our cyber networks safe.

In addition, DHS works closely with international partners to enhance information sharing, increase situational awareness, improve incident response capabilities, and coordinate strategic policy issues in support of the Administration's International Strategy for Cyberspace. For example, the Department has fostered international partnerships in support of capacity building for cybersecurity through agreements with Computer Emergency Response and Readiness Teams as well as the DHS Science & Technology Directorate (S&T). Since 2009, DHS has established partnerships with Australia, Canada, Egypt, India, Israel, the Netherlands, and Sweden.

Fostering Innovation

The Federal Government relies on a variety of stakeholders to pursue effective research and development projects that address increasingly sophisticated cyber threats. This includes research and development activities by the academic and scientific communities to develop capabilities that protect citizens by enhancing the resilience, security, integrity, and accessibility of information systems used by the private sector and other critical infrastructure. DHS supports Centers of Academic Excellence around the country to cultivate a growing number of professionals with expertise in various disciplines, including cybersecurity. DHS S&T is leading efforts to develop and deploy more secure internet protocols that protect consumers and industry internet users. We continue to support leap-ahead research and development, targeting revolutionary techniques and capabilities that can be deployed over the next decade with the potential to redefine the state of cybersecurity in response to the Comprehensive National Cybersecurity Initiative. For example, DHS was a leader in the development of protocols at the Internet Engineering Task Force called Domain Name System Security (DNS SEC) Extensions. DNS SEC is necessary to protect internet users from being covertly redirected to malicious websites and helps prevent theft, fraud, and abuse online by blocking bogus page elements and flagging pages whose Domain Name System (DNS) identity has been hijacked. S&T is also driving improvements through a Transition to Practice Program as well as liability and risk management protections provided by the Support Anti-Terrorism by

Fostering Effective Technology (SAFETY) Act that promote cyber security technologies and encourage their transition into successful use.

Growing and Strengthening our Cyber Workforce

We know it only takes a single infected computer to potentially infect thousands and perhaps millions of others. But at the end of the day, cybersecurity is ultimately about people. The most impressive and sophisticated technology is worthless if it's not operated and maintained by informed and conscientious users.

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.

Recent Executive Actions

As discussed above, 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 government's role in this effort is to share information and encourage enhanced security and resilience, while identifying and addressing gaps not filled by the market-place.

Last month, President Obama issued Executive Order 13636 on Improving Critical Infrastructure Cybersecurity as well as Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, which will 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.

DHS Responsibilities

The President's actions mark an important milestone in the Department's ongoing efforts to coordinate the national response to significant cyber incidents while enhancing the efficiency and effectiveness of our work to strengthen the security and resilience of critical infrastructure. The Executive Order supports more efficient sharing of cyber threat information with the private sector and directs NIST to develop a Cybersecurity Framework to identify and implement better security practices among critical infrastructure sectors. The Executive Order directs DHS to establish a voluntary program to promote the adoption of the Cybersecurity Framework in conjunction with Sector-Specific Agencies and to work with industry to assist companies in implementing the framework.

The Executive Order also expands the voluntary DHS Enhanced Cybersecurity Service program, which promotes cyber threat information sharing between government and the private sector. This engagement helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely. This program is a good example of information sharing with confidentiality, privacy and civil liberties protections built into its structure. DHS will share with appropriately cleared private sector cybersecurity providers the same threat indicators that we rely on to protect the .gov domain. Those providers will then be free to contract with critical infrastructure entities and provide cybersecurity services comparable to those provided to the U.S. Government.

Through the Executive Order, the President also directed agencies to incorporate privacy, confidentiality, and civil liberties protections. It specifically instructs DHS to issue a public report on activities related to implementation, which would therefore enhance the existing privacy policy, compliance, and oversight programs of DHS and the other agencies.

In addition, the Presidential Policy Directive directs the executive branch to strengthen our capability to understand and efficiently share information about how well critical infrastructure systems are functioning and the consequences of potential failures. It also calls for a comprehensive research and development plan for critical infrastructure to guide the government's effort to enhance market-based innovation.

Because the vast majority of U.S. critical infrastructure is owned and operated by private companies, reducing the risk to these vital systems requires a strong partnership between government and industry. There is also a role for state, local, tribal and territorial governments who own a significant portion of the nation's critical infrastructure. In developing these documents, the Administration sought input from stakeholders of all viewpoints in industry, government, and the advocacy community.

Their input has been vital in crafting an order that incorporates the best ideas and lessons learned from public and private sector efforts while ensuring that our information sharing incorporates rigorous protections for individual privacy, confidentiality, and civil liberties. Indeed, as we perform all of our cyber-related work, we are mindful of the need to protect privacy, confidentiality, and civil liberties. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset. To accomplish the integrated implementation of these two directives, DHS has established an Interagency Task Force made up of representatives from across all levels of government.

Continuing Need for Legislation

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.

The Administration's legislative priorities for the 113th Congress build upon the President's 2011 Cybersecurity Legislative Proposal and take into account two years of public and congressional discourse about how best to improve the nation's cybersecurity. Congress should enact legislation to incorporate privacy, confidentiality, and civil liberties safeguards into all aspects of cybersecurity; strengthen our critical infrastructure's cybersecurity by further increasing information sharing and promoting the establishment and adoption of standards for critical infrastructure; give law enforcement additional tools to fight crime in the digital age; and create a National Data Breach Reporting requirement.

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 look forward to working with this Committee and the Congress to ensure we continue to take every step necessary to protect cyberspace, in partnership with government at all levels, the private sector, and the American people, and continue to build greater resiliency into critical cyber networks and systems.

I appreciate this Committee's guidance and support as together we work to keep our nation safe. Thank you, again, for the attention you are giving to this urgent matter.