Statement for the Record
Of

Acting Assistant Secretary Roberta Stempfley

and

Director Lawrence Zelvin, National Cybersecurity and Communications Integration Center

Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security
Washington, DC

May 16, 2013

Introduction

Chairman Meehan, Ranking Member Clarke, and distinguished Members of the Committee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC). Specifically, I will discuss the NCCIC's role, responsibilities, and future planning to protect our Nation's critical infrastructure from cyber attacks, secure Federal networks, and coordinate private sector cyber threat information sharing.

Before I begin, I would like to thank the Committee for its leadership during the recent legislative debate over the Cyber Intelligence Sharing and Protection Act, especially in support of passing an amendment to designate DHS as the lead civilian Federal entity to receive cyber threat information. Cybersecurity threats put the confidentiality, integrity, and availability of critical services at risk. DHS, along with its government and private sector partners, works to counter these threats while supporting a cyber ecosystem that is open, transparent, and less vulnerable to manipulation. The NCCIC supports this effort by providing comprehensive and robust information sharing, incident response, technical assistance, and analysis capabilities to private sector, government, and international partners.

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 communicating, traveling, powering our homes, running our economy, and obtaining government services. No country, industry, community or individual is immune to cyber risks.

The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Cyber crime also has increased significantly over the last decade. Sensitive information is routinely stolen from private sector and government networks, undermining the integrity of the data contained within these systems. The Department currently sees malicious cyber activity from foreign nations and non-state actors engaged in intellectual property theft and information operations, 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 remote access, thumb drives, supply chain exploitation, and leveraging trusted insiders' access.

The Department has seen motivations for attacks vary from intellectual property theft to criminals seeking financial gain and hackers who may seek bragging rights in the hacker community. Industrial control systems also are targeted by a variety of malicious actors who may have intentions to damage equipment and facilities or steal data. Foreign actors also are 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.

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively provide for 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. To achieve a whole-of-Government response, DHS, DOJ, and DOD coordinate continuously to effectively respond to specific incidents. 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."

NCCIC's Cybersecurity Mission

DHS coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure by ensuring maximum coordination and partnership with the private sector while ensuring that privacy, confidentiality, and civil rights and civil liberties are not diminished by its security initiatives. Accordingly, the Department has implemented rigorous privacy and civil rights and civil liberties standards, which apply to all of its cybersecurity programs and initiatives. In order to protect privacy while safeguarding and securing cyberspace, DHS institutes layered privacy responsibilities throughout the Department, embeds fair information practice principles into cybersecurity programs and privacy compliance efforts, and fosters collaboration with cybersecurity partners.

Within DHS's National Protection and Programs Directorate (NPPD), the Office of Cybersecurity and Communications (CS&C) focuses on managing risk to the communications and information technology infrastructures and the sectors that depend upon them, as well as enabling timely response and recovery of these infrastructures under all circumstances. CS&C executes its mission by supporting 24x7 information sharing, analysis, and incident response; facilitating interoperable emergency communications; advancing technology solutions for private and public sector partners; providing tools and capabilities to ensure the security of Federal civilian executive branch networks; and engaging in strategic level coordination for the Department with private sector organizations on cybersecurity and communications issues.

To better manage and facilitate cybersecurity information sharing efforts, analysis, and incident response activities, the Department established the NCCIC, a round-the-clock information sharing, analysis and incident response center where government, private sector, and international partners all work together. The NCCIC is comprised of four branches: the United States Computer Emergency Readiness Team (US-CERT), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center for Telecommunications (NCC), and Operations Integration (O&I). As mutually supporting and integrated elements of the NCCIC, these branches provide the unique authorities, capabilities, and partnerships needed to drive a whole-of-nation approach to addressing cybersecurity and communications issues at the operational level.

- US-CERT provides advanced information sharing, incident response, and analysis expertise for malicious cyber activity targeting private sector and government networks. US-CERT's global partnerships allow it to work directly with analysts from across multiple sectors and international borders to develop a comprehensive picture of malicious activity and mitigation options. US-CERT's mission focuses specifically on computer network defense, and it is able to apply its full resources to supporting prevention, protection, mitigation, response, and recovery efforts.

- ICS-CERT reduces risk to the Nation's critical infrastructure by strengthening the cybersecurity of systems that operate our Nation's critical infrastructure. It carries out this mission by performing incident response to support asset owners with discovery, analysis and recovery efforts as well as providing situational awareness through training, alerts, and advisories to warn of cyber based threats and vulnerabilities affecting critical infrastructure assets. In addition, ICS-CERT conducts assessments and technical analysis of malware, digital media, system vulnerabilities, and emerging exploits and partners with the control systems community to coordinate risk management activities.

- NCC leads and coordinates the initiation, restoration, and reconstitution of the National Security/Emergency Preparedness (NS/EP) telecommunications services or facilities during any human-caused or natural event where physical communications infrastructure is damaged or vulnerable. NCC leverages partnerships across government, industry and international partners to gain situational awareness and determine priorities for protection and response. NCC's presence in the NCCIC allows DHS to synchronize operational processes supporting both the physical and the virtual components of our Nation's information and communications technology infrastructure.

- O&I applies planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident response efforts, ensuring effective synchronization across the NCCIC.

Strategic Goals

The NCCIC works to proactively analyze cybersecurity and communications threats and vulnerabilities and coordinate their findings with partners to manage risks to critical systems; create shared situational awareness among public sector, private sector, and international partners by collaboratively developing and sharing timely and actionable cybersecurity and communications information; and rapidly respond to routine and significant cybersecurity and communications incidents and events to mitigate harmful activity, manage crisis situations, support recovery efforts, and assure NS/EP.

To accomplish its strategic goals, NCCIC relies on the voluntary coordination, collaboration, capabilities, and resources of its partners. The center works closely with those Federal agencies most responsible for securing the Government's cyber and communications systems, including the Departments of Treasury and Energy. The NCCIC also actively engages with the appropriate private sector entities, information sharing and analysis centers, state, local, tribal, and territorial governments, and international partners. As integral parts of the cyberspace and communications community, these groups work together to protect the portions of critical information technology that they interact with, operate, manage, or own. These groups of stakeholders represent natural communities of practice providing the foundation for effective information sharing and response.

<u>Threat Analysis</u>

NCCIC collaborates with private sector, government, and international partners to identify, research, and verify suspicious, malicious, or potentially harmful cybersecurity and communications activity, events, or incidents. For example, US-CERT operates NCCIC's Advanced Malware Analysis Center, which receives malware samples and other potentially malicious files from around the world. The Advanced Malware Analysis Center analyzes those files, shares that analysis broadly to alert partners to malicious activity, and provides them with actionable indicators and recommendations to improve their ability to protect themselves.

By understanding the nature of attacks, vulnerabilities, and risks, NCCIC is able to determine possible impacts, set priorities, and proactively develop and share effective mitigation strategies. NCCIC strives to anticipate potentially harmful activity and provide actionable alert and warning information to partners before they are impacted. NCCIC's analysis efforts, whether focused on a new piece of malware or a tropical storm with the potential to damage critical communications systems, contribute directly to its information sharing, response, and protection and prevention capabilities.

Situational Awareness

The success of the NCCIC's mission is heavily reliant on its ability to establish shared situational awareness of potentially harmful activity, events, or incidents across multiple constituencies to improve the ability of diverse and distributed partners to protect themselves. To do this, NCCIC integrates analysis and data received through its own analysis, intelligence community and law enforcement reporting, and data shared by private sector and international partners into a comprehensive series of actionable information products, which are shared with partners in easy to digest machine-readable formats.

Multidirectional sharing of alerts, warnings, analysis products, and mitigation recommendations among Federal, state, local, tribal, and territorial governments, private sector, including information sharing and analysis centers, and international partners is a key element of NCCIC's cyber and communications protection and prevention framework. The NCCIC continuously works with a broad range of partners to explore and innovate new ways to enhance information sharing and move closer to network speed communications.

Rapid Response

The NCCIC applies the collective capabilities of its partners and constituents to identify, prioritize, and escalate confirmed cybersecurity incidents in order to minimize impacts to critical information infrastructure. To ensure a 24x7 capability, NCCIC maintains cross functional incident response teams, which draw from the capabilities of NCCIC's branches, along with expertise from elsewhere in DHS such as the United States Secret Service (USSS) and Immigration and Customs Enforcement (ICE). Working under a voluntary request for technical assistance, these incident response teams analyze malware, review network logs, and assess security posture to identify possible malicious activity, its impacts, as well as mitigation and recovery options.

Recognizing the possibility of a cyber incident with physical impacts or a physical incident with cyber implications, NCCIC works increasingly closely with NPPD's National Infrastructure Coordinating Center (NICC). This collaboration, directed by Presidential Policy Directive 21 (PPD-21), helps to ensure strong synchronization between DHS's infrastructure protection efforts in both the cyber and physical realms. In addition, the NCCIC assists in the initiation, coordination, restoration, and reconstitution of the NS/EP telecommunications services or facilities under all conditions, crises, or emergencies including executing Emergency Support Function 2 – Communications responsibilities under the National Response Framework.

These efforts provide a whole-of-nation approach to incident response, efficiently and effectively leveraging capabilities from across DHS's partner base while implementing key policies.

Protecting Critical Infrastructure

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 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, and through collaboration between the NCCIC and the NICC, integrates efforts across the physical and cyber domains. The Department also conducts onsite risk assessments of critical infrastructure and shares risk and threat information with state, local and private sector partners. NCCIC 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. These efforts provide unique value to private sector partners by integrating data from companies and industries that might not normally communicate.

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. Through the CISCP, participating private sector partners are able to share data directly with government. When requested, these datasets are covered by the Protected Critical Infrastructure Information (PCII) program, which protects the name of the company that shared the information from disclosure through Freedom of Information Act requests, regulatory processes, civil litigation, and other sunshine law requirements. Submitted datasets are analyzed in the context of other data received from across sectors, and based on this analysis regular analytical products are shared back out with partners. CISCP has signed 40 Cooperative Research and Development Agreements (CRADAs), and is in the process of finalizing agreements with 66 additional entities to formalize a streamlined information sharing process. Since December 2011, CISCP has released over 900 products containing approximately 18,000 cyber threat indicators, which are based on information the Department has gleaned from participant submissions, open source research, and from sensitive government information.

NCCIC has also benefited from close collaboration with the USSS and ICE, which have complementary jurisdiction over the investigation of computer crime violations that they exercise to protect the Nation’s leaders and critical infrastructure and strategically target transnational organized criminals who are exploiting the financial system through cybercrimes. By working closely together, NCCIC and its law enforcement partners are able to leverage each organization’s expertise and unique authorities to more effectively and efficiently execute DHS’s cybersecurity mission.

Responding to Cyber Threats

As the civilian Department at the intersection of public-private information sharing, DHS is a focal point for coordinating cybersecurity information sharing with the private sector, the Department engages with owners and operators, based on their requests for technical assistance, by providing onsite analysis, mitigation support, and assessment assistance. The Department has repeatedly demonstrated its ability to expeditiously support private sector partners with cyber intrusion mitigation and incident response. Initiating technical assistance with any private company to provide analysis and mitigation advice is a sensitive endeavor that requires trust and strict confidentiality. DHS’s efforts focus on civilian computer network defense and protection rather than law enforcement, military, or intelligence functions in order to mitigate threats to the networks and reduce future risks.

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. In 2012, US-CERT processed approximately 190,000 cyber incidents involving Federal agencies, critical infrastructure, and the Department's 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 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, which includes analyzing data and sharing results, developing mitigation recommendations, and providing alerts and warning to potential future victims. DHS also empowers owners and operators through a cyber self-evaluation tool, the Cyber Security Evaluation Tool (CSET®), which was used by over 1,000 companies last year. In addition, DHS provides in-person and on-line training sessions that focus on network security.

The NCCIC, and its Federal partners, works with the private sector and international partners in preventing intellectual property theft with a whole-of-Government approach. For example, the United States Secret Service – which brings together over 6,000 partners from across sectors through its 29 domestic Electronic Crimes Task Forces (ECTFs) - investigates cyber crimes within its jurisdiction, and the United States Coast Guard contains a component of U.S. Cyber Command and U.S. Strategic Command for the conduct of military missions. In each case, DHS focuses not only on responding to the incident at hand, but also on identifying trends, warning potential victims, and proactively engaging with partners. DHS, in collaboration with FBI and other partners, released a series of Joint Indicator Bulletins, containing cyber threat indicators to help private sector partners take action to stop this activity and protect them from theft of intellectual property, trade secrets and sensitive business information.

Most recently, and in close collaboration with interagency partners as well as industry partners like the Financial Services Information Sharing and Analysis Center,DHS has been engaged with private sector and international partners during the series of DDoS incidents over the past few months. DHS has provided technical data and assistance, including identifying hundreds of thousands of DDoS related IP addresses and supporting contextual information in order to help financial institutions and their information technology security service providers improve their defensive capabilities. In addition to sharing with these private sector entities, DHS has provided this information to over 120 international partners, many of whom have contributed to our mitigation efforts. DHS, along with the FBI and other interagency partners, has also deployed on-site technical assistance to provide in person support, and has conducted numerous classified briefings on the nature of the threat and mitigation strategies to hundreds of financial sector IT security specialists. These efforts have helped to increase the U.S. Government's sharing and coordination efforts internally and with private sector partners. Additionally, the mitigation strategies provided have not only helped financial institutions significantly blunt the impact of these attacks, but they have also helped the industry develop new strategies of their own that DHS hopes to share with other sectors of critical infrastructure to help mitigate similar attacks.

NCCIC's NCC played a vital role in response to Hurricane Sandy recovery efforts. The NCC, as the coordinator for Emergency Support Function #2 under the National Response Framework, provided a wide range of communications support in partnership with industry to support responders, citizens, and industry response and recovery. NCC worked to improve first responder actions by assisting in radio network infrastructure restoration such as microwave connectivity supporting local fire department dispatch and coordination. They also coordinated aid to citizens through more than 170 instances of emergency provisioning of communications installations supporting response organizations such as the American Red Cross, Army Corps of Engineers, Social Security Administration, and the Federal Emergency Management Agency. Collaborating with industry, NCC enhanced wireless coverage to first responders who provide emergency services to approximately 33,400 citizens in Long Beach, New York; 1,400,000 citizens in Nassau County and 130,000 citizens in Far Rockaway, Queens. Their efforts also supported the recovery of communications to the U.S. financial sector by coordinating fuel and power restoration to a key facility in New York City, ensuring no impact to international financial trading.

Finally, in March 2012, DHS identified a campaign of cyber intrusions targeting natural gas pipeline sector companies with spear-phishing e-mails that dated back to December 2011. The attacks were 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. While there is no evidence that anyone has tried to subvert the operation of these industrial control systems, the intent of the attacker remains unknown. DHS immediately began an action campaign to alert the oil and natural gas pipeline sector community of the threat and offered to provide assistance. Industry partners have been responsive to these threats, and in May and June 2012, DHS deployed onsite assistance to two of the organizations targeted in this campaign: an energy company that operates a gas pipeline in the U.S. and a manufacturing company who specializes in producing materials specific to pipeline construction. DHS also partnered with the Department of Energy and others to conduct briefings across the country. Over 500 private sector individuals attended the classified briefings and hundreds more received unclassified briefings providing warnings and mitigation strategies.

Recent Executive Actions

As today's physical and cyber infrastructures become increasingly linked, critical infrastructure and emergency response functions grow ever more 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. These policies work in conjunction with Executive Order 13618 of July 6, 2012, Assignment of National Security and Emergency Preparedness Communications

Functions, which improves how the Executive Branch handles NS/EP Communications and ties cyber into emergency response communications.

In February 2013, President Obama issued EO 13636, as well as PPD-21 on Critical Infrastructure Security and Resilience, which will work 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, and will improve NCCIC's ability to execute its mission in support of the private sector. 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, and these policies will further enable NCCIC's mission. EO 13636 supports more efficient sharing of cyber threat information with the private sector and directs the National Institute of Standards and Technology to develop a Cybersecurity Framework to identify and implement better security practices among critical infrastructure sectors. EO 13636 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.

EO 13636 also expands the DHS Enhanced Cybersecurity Services (ECS) program, key aspects of which are operated by the NCCIC. ECS is 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 USG 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 (CSPs) that will enable them to better protect their customers who are critical infrastructure entities. CSPs can deliver approved services to validated critical infrastructure entities through commercial relationships. The ECS program is not involved in establishing commercial relationships between CSPs and CI entities. ECS augments, but does not replace, entities' existing cybersecurity capabilities. The ECS information sharing process protects Critical Infrastructure (CI) entities against cyber threats that could otherwise harm their systems. ECS program participation is voluntary and designed to protect government intelligence, corporate information security, and the privacy of participants, while enhancing the security of critical infrastructure. Validated CI entities from all 16 CI sectors are eligible to participate in the ECS program and receive ECS services from an eligible CSP.

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 calls for a comprehensive research and development plan for critical infrastructure to guide the Government's effort to enhance market-based innovation. The strategic imperatives in PPD-21 also direct the NCCIC and the NICC to "function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure." As such, NPPD is enhancing the existing coordination of its two critical infrastructure operations centers, the NCCIC and the NICC.

Continuing Need for Legislation

We continue to believe that carefully crafted information sharing provisions, as part of a comprehensive suite of cybersecurity legislation, are essential to improve the Nation's cybersecurity to an acceptable level, 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

Set within an environment characterized by a dangerous combination of known and unknown vulnerabilities, rapidly evolving adversary capabilities, and a lack of comprehensive threat and vulnerability awareness, the cybersecurity mission is truly a national one requiring broad collaboration. DHS is committed to creating a safe, secure, and resilient cyber environment while promoting cybersecurity knowledge and innovation and protecting privacy, confidentiality, civil rights and civil liberties in collaboration with its public, private, and international partners. Thank you for your continued support and attention to the critical issue of cybersecurity and I look forward to your questions.