"Cyber Incident Response: Bridging the Gap between Cybersecurity and Emergency Management"

Statement for the Record

Roberta Stempfley
Acting Assistant Secretary for Cybersecurity and Communications
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Emergency Preparedness, Response, and Communications

and

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

Washington, DC
October 30, 2013

Chairwoman Brooks and Chairman Meehan, Ranking Members Payne and 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) coordination with state, local, tribal, and territorial (SLTT) emergency managers on cybersecurity issues. This October marks the 10th anniversary of National Cyber Security Awareness Month, which is an opportunity to further engage public and private sector stakeholders to create a safe, secure, and resilient cyber environment. Everyone has a role to play in cybersecurity and I am pleased to discuss the Department's efforts to engage SLTT emergency managers as they build cybersecurity resilience into those networks and systems upon which they depend on a daily basis.

America's cybersecurity is inextricably linked to our nation's economic vitality – IT systems are interdependent, interconnected and critical to our daily lives – from communication, travel, and powering our homes, to running our economy, and obtaining government services. 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, which include the nation's physical and cyber infrastructure. We are also 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.

Cybersecurity Support to SLTT Emergency Managers

Protecting this infrastructure against growing and evolving cyber threats requires a layered approach. 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 marketplace. Providing effective cybersecurity services requires fostering relationships with those who own and operate the communications infrastructure, members of the emergency responder community, and Federal, state, local, tribal, and territorial partners. Indeed, as many of the communications technologies currently used by public safety and emergency services organizations move to an Internet Protocol (IP)-based environment, there is an increase in the cyber vulnerabilities of our emergency services providers in the conduct of their mission. It is important, therefore, for the Department to engage not just Chief Information Officers (CIO) or Chief Information Security Officers (CISO) at the SLTT level, but also the emergency managers and other officials for whom a secure cyber environment is equally as important to accomplishing their mission.

The Department has initiated several activities focused on ensuring SLTT emergency managers are able to build cybersecurity resilience into those information and technology networks and systems upon which they depend. Cyber dependencies and interdependencies require interactions between several different DHS organizations and SLTT partners in order to address this complex need. DHS has been forward-thinking as the reliance upon cyber systems has grown and our engagements have been ongoing.

Previous Efforts

- ***Regionally-Based Cybersecurity Advisors.*** The Cybersecurity Advisors (CSA) program was created and implemented by CS&C in 2010. The regionally-deployed personnel promote cybersecurity awareness, program and policy coordination, information sharing, and risk analysis to their partners, including emergency managers. Over the last year, CSAs have had direct engagement with 13 state or local emergency centers. In addition, the Department has conducted Cyber Resilience Reviews and assessments and provided support to numerous National Security Special Events, including planning for events such as the Super Bowl, and the G8 with the City of Chicago's Office of Emergency Management & Communications.

- ***Emergency Services Sector Cyber Risk Assessment***. Encompassing a wide range of emergency response functions carried out by five disciplines[1], in 2012 the Emergency Services Sector completed a Cyber Risk Assessment, which provides a risk profile to enhance the security and resilience of the Emergency Services Sector disciplines. It is an effort to establish a baseline of cyber risks across the sector, to ensure Federal resources are applied where they offer the most benefit for mitigating risk, and to encourage a

[1] Law Enforcement; Fire and Emergency Services; Emergency Management; Emergency Medical Services; and Public Works

similar risk-based allocation of resources within state and local entities and the private sector. Emergency managers from local, state, and Federal government actively participated in the development process to ensure the assessment provided practical guidance for the public safety community. The Department continues to meet with officials from stakeholder associations such as the National Emergency Management Association to discuss next steps, including developing a workforce training program for emergency managers in order to increase cybersecurity capabilities within the emergency management community.

- ***Local Pilot Projects with Emergency Managers and Critical Infrastructure Partners.*** DHS is conducting three pilots to better understand the interconnections between cyber and physical infrastructure and the potential risks to the nation. The first pilot, initiated in 2012, worked closely with Charlotte, NC emergency planners and neighboring communities to examine how a potential cyber attack could disrupt communications or other infrastructure operations. The work provided additional ways for planners to mitigate potential cyber impacts and, as a result of the pilot, commercial facilities adopted additional security practices to shore up potential weaknesses.

  The second pilot is underway with the State of New Jersey examining the interrelationship between IT, communications and physical security. The pilot involves five water and wastewater facilities and has received praise from the State Office of Homeland Security and our water sector partners. As a result of initial findings, water facilities have taken immediate action to mitigate previously unknown vulnerabilities.

  The third pilot is a joint cyber-physical assessment of a Federal facility in Washington, DC to develop a common approach for identifying cyber security vulnerabilities affecting security systems of federally protected facilities, including electrical, HVAC, water, telecommunications, and security control systems.

  The lessons from these pilots have been incorporated into our integrated physical and cyber Regional Resiliency Assessment Program (RRAP). This is helping strengthen the partnership we already have; build new relationships between SLTT CIOs, first responders, and critical infrastructure owners and operators; and lay the foundation increased collaboration to increase cybersecurity resilience.

- ***Nationwide Public Safety Broadband Network (NPSBN) Cyber Infrastructure Risk Assessment***. The development and deployment of an IP-based network for public safety will represent a leap forward in communications capabilities for first responders, law enforcement, and other users of the NPSBN. However, the move to such a network presents a challenge for the emergency management community to identify threats to and vulnerabilities of cyber infrastructure in the NPSBN that could affect the network's reliability and security. DHS is working with the First Responder Network Authority (FirstNet) and the public safety community to identify cyber risks and develop potential responses to those risks. In 2013, OEC developed the NPSBN Cyber Infrastructure Risk

Assessment to provide FirstNet with a how-to guide to address the top cyber risks that the network may face, and is now working with FirstNet to ensure a more resilient network design that will integrate security and resilience into the overall physical and cyber aspects of the NPSBN.

- **Cyber Threat Information Sharing**
  In June 2013, DHS established "sharelines" in compliance with Executive Order (EO) 13636 and Presidential Policy Directive (PPD) -21 to help increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities, to include SLTT owners and operators, so that these entities may better protect and defend themselves against cyber threats. Sharelines "facilitate the creation and dissemination of unclassified cyber threat reports to targeted private sector entities owned or operating within the United States, as well as Federal, State, local, tribal, and territorial partners" in a timely manner.

Ongoing Efforts

DHS continues to build upon the relationships we have established throughout the Emergency Services Sector through strategic and operational efforts to provide solutions to our SLTT partners. Ongoing efforts within DHS consist of:

- ***Update to the National Emergency Communications Plan.*** DHS is updating the National Emergency Communications Plan (NECP) in coordination with the public safety community to enhance planning, preparation, and security of broadband technologies used during response operations. The Plan will discuss how cybersecurity has become a key consideration for public safety officials as new IP-enabled technology is increasingly integrated into operations. The NECP will endorse a multifaceted approach to ensure the confidentiality, integrity, and availability of sensitive data. For example, comprehensive cyber training and education on the proper use and security of devices and applications, phishing, malware, other potential threats, and how to stay on guard against attacks will be recommended.

- ***9-1-1 Centers: Next Generation 9-1-1 and Telephonic Denial of Service.*** Updated 9-1-1 infrastructure utilizes public voice, data, and video capabilities, which introduce new vulnerabilities into 9-1-1 systems. Separately, 9-1-1 centers have been targeted by telephonic denial of service (TDOS) attacks that overwhelm Public Safety Answering Points' administrative lines. These attacks inundate a 9-1-1 call center with a high volume of calls, overwhelming the system's ability to process calls and tying up the system from receiving legitimate calls. DHS, through the NCCIC, has worked on the development and dissemination of techniques for mitigating and managing these TDOS attacks in order to allow emergency management agencies to continue to provide these critical services to the public.

- ***Protective Security Advisors (PSAs).*** Within the Office of Infrastructure Protection, PSAs serve as the nexus of our infrastructure security and coordination efforts at the Federal, state, local, tribal, and territorial levels and serve as DHS's onsite critical infrastructure and vulnerability assessment specialists. PSAs have also been working with CS&C to better coordinate assessments and as a result approximately half of cybersecurity site assessments administered by CS&C were conducted in tandem with PSAs—an example of how we are working to better and more effectively integrate our physical and cyber security efforts across NPPD and the Department.

- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**
  DHS builds partnerships with non-federal public sector stakeholders to protect critical network systems. For example, the Multi-State Information Sharing and Analysis Center (MS-ISAC) opened its Cyber Security Operations Center in November 2010, which has enhanced the National Cybersecurity & Communications Integration Center (NCCIC) situational awareness at the state and local government level and allows the Federal Government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments. Since 2009, the NCCIC has responded to nearly a half a million incident reports and released more than 26,000 actionable cybersecurity alerts to our public and private sector partners.
  Membership in the MS-ISAC consists of state and local CISOs and other leadership from all 50 state governments, the District of Columbia, 373 local governments, three territories, five tribes, and 24 educational institutions. It provides valuable information and lessons learned on cyber threats, exploitations, vulnerabilities, consequences, incidents and direct assistance with responding to and recovering from cyber-attacks and compromises. The MS-ISAC runs a 24-hour watch and warning security operations center that provides real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach aimed to reduce risk to the Nation's SLTT government cyber domain. This year the MS-ISAC developed a plan to increase engagement with emergency managers and fusion centers.

Operational Efforts

Assuring the security and reliability of critical information networks is vital across all critical infrastructure sectors, including the Emergency Services Sector, which is charged with saving lives, protecting property and the environment, assisting communities impacted by disasters, and aiding recovery from emergencies. DHS is uniquely positioned to improve the cybersecurity posture of our stakeholders.

National Protection and Programs Directorate

The Offices of the National Protection Programs Directorate interact daily with state and local officials and emergency managers on communications and cybersecurity issues to strengthen infrastructure, educate citizens, and respond to and recover from online threats and attacks.

- **Cybersecurity and Communications**
  CS&C maintains an overall focus on reducing risk to the communications and information technology infrastructures and the sectors that depend upon them, as well as providing threat and vulnerability information and enabling timely response and recovery of these infrastructures under all circumstances. We execute our mission by supporting 24x7 information sharing, analysis, and incident response through the National Cybersecurity Communications Integration Center (NCCIC); facilitating interoperable emergency communications through our Office of Emergency Communications (OEC); 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 stakeholders on cybersecurity and communications issues. Additionally OEC has strong ties to emergency managers through its outreach to State Wide Interoperability Coordinators (SWIC) who state officials who are the primary points of contact for communications interoperability issues. These produce State Wide Interoperability Plans which establish governance, processes, and procedures to support first responder communication. These strong relationships also help SLTT leverage other resources such as fusion centers.

- **Office of Infrastructure Protection**
  The Office of Infrastructure Protection within NPPD leads and coordinates national programs and policies on critical infrastructure, including through implementation of the National Infrastructure Protection Plan (NIPP). The NIPP establishes the framework for integrating the Nation's various critical infrastructure protection and resilience initiatives into a coordinated effort, and provides the structure through which DHS, in partnership with Government and industry, implements programs and activities to protect critical infrastructure, promote national preparedness, and enhance incident response. As the NIPP is updated based on the requirements of Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, NPPD will work with critical infrastructure stakeholders to focus the revision on enhanced integration of cyber and physical risk management, requirements for increased resilience, and recognition for the need for enhanced information sharing and situational awareness. As we work to update the NIPP we will support the Emergency Services Sector to ensure that we inform first responders in their preparation for cyber incidents

Coordinated Cyber/Physical Response

While the National Cybersecurity Communications Integration Center (NCCIC) processes incident reports, issues actionable cybersecurity alerts, and deploys onsite incident response fly-away teams to critical infrastructure organizations to assist with analysis and recovery efforts of a cyber incident, the National Infrastructure Coordinating Center (NICC) provides situational awareness of threats to physical critical infrastructure, incident response support and business reconstitution assistance. In addition to this coordination, as incidents or threats occur, PSAs

living in communities across the country provide the Department with a 24/7 capability to assist in developing a common operational picture for critical infrastructure. NPPD efforts to integrate physical and cyber security have provided benefits during incidents including:

- **Hurricane Sandy:** NPPD operational efforts were able to facilitate much-needed fuel deliveries to critical telecommunication sites in lower Manhattan in order to fuel generators and keep the facilities operational in recent events like Hurricane Sandy. After PSAs were notified of the fuel supply shortage, NPPD provided analysis on the wide-spread impact if the telecommunications facility lost power, while the NCCIC worked with its public and private sector partners to identify a fuel supply and coordinate its delivery to the critical site.

- **Boston Marathon Bombing:** OEC worked closely with public safety agencies in the Metro Boston Homeland Security Region and with the Commonwealth of Massachusetts on several key emergency communications initiatives prior to the 2013 marathon including observing public safety communications during previous marathons and events and offering suggestions to help strengthen the region's capabilities and improve coordination. Three years later, DHS saw many of the recommendations from this assessment in action in response to the bombings, including the region's use of a detailed communications plan (ICS Form 205) for the event that assigned radio channels to various agencies and functions.

Conclusion

DHS provides a variety of services and capabilities designed to support emergency managers at all levels of engagement, across education, planning, cyber-incident response, and recovery activities. The services and capabilities are all integral parts of reducing risk and building capacity of our SLTT partners. As necessary, those relationships are leveraged in operational response efforts in order to meet immediate, critical needs. As technologies continue to advance and the dependencies and interdependencies between the sectors and systems continue to advance along with them, DHS will continue to work with emergency managers in a holistic fashion to plan, prepare, mitigate and build resilience into those information and technology networks and systems upon which they depend on a daily basis. Thank you for this opportunity to testify, and I look forward to answering any questions you may have.