

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

**Testimony of Roberta Stempfley
Acting Assistant Secretary
Office of Cybersecurity and Communications
National Protection and Programs Directorate
Department of Homeland Security**

**Before the
United States House of Representatives
Energy and Commerce Committee
Subcommittee on Communications and Technology
Washington, DC**

March 28, 2012

**Hearing on
Cybersecurity of Communications Networks**

Chairman Walden, Ranking Member Eshoo, and distinguished members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) efforts to secure communications networks. Before I begin, I would like to thank the Committee members for their leadership and dedication to supporting enactment of legislation to create a Nationwide Public Safety Broadband Network. As you know, this was one of the 9/11 Commission recommendations and one of the Administration's priorities over the last year. We look forward to continuing to work with the Committee to implement these efforts and build a nationwide, interoperable network for emergency responders.

In addition to our emergency communications work with public safety agencies, the Department works closely with the communications industry to ensure a resilient, reliable, and available communications infrastructure. Today I will provide an overview of the communications infrastructure, the Department's mission as it relates to the protection of the communications infrastructure, and the coordination of this mission with our public- and private-sector partners.

As communications technology evolves, the Federal Government must also evolve. The Government must make advances alongside industry to ensure that the Government has access to tools that allow it to communicate internally and with the public in all circumstances. It is also critical that as communications technology evolves, this advancement includes appropriate security. Accomplishing this goal requires the Federal Government to develop strategies to address challenges inherent in emerging, and often game-changing, technologies. Public safety agencies are increasingly relying on these emerging technologies. Further, the Nation's newfound reliance on mobile devices and applications, as well as on social networking tools, to communicate presents both opportunities and challenges. Because the private sector owns much of the Nation's

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

infrastructure, protecting it is a responsibility that the Federal Government cannot, and should not, shoulder alone. Instead, we must collaborate closely with our public- and private-sector partners.

The Communications Infrastructure

Access to a reliable and resilient communications network is essential to maintaining the Nation's health, safety, economy, and public confidence. As such, protection of the communications infrastructure from threats of natural disasters, cyber attacks, and terrorism is among the Department's highest priorities. The Department has committed resources to addressing this.

The Nation's communications network is a complex system of systems, which incorporates multiple technologies and services with diverse ownership. This infrastructure includes wireline, wireless, satellite, cable, broadcasting capabilities, and the transport networks that support the Internet and other key information systems the Government depends upon every day. The communications companies that own, operate, and supply the Nation's communications infrastructure have historically factored natural disasters and intentional and accidental disruptions into network resilience architecture, business continuity plans, and disaster recovery strategies. As the industry transitions from point-to-point (circuit switch) to router-to-router (packet switch) technologies, DHS continues working with private-sector companies to implement strategies critical to protecting the infrastructure.

The interconnected and interdependent nature of these service-provider networks has for decades fostered crucial information sharing and cooperative response-and-recovery relationships. Even in today's highly competitive business environment, the community has a long-standing tradition of cooperation and trust, which is imperative because problems with one service provider's network inevitably impact the other providers.

Providing coordinated and collaborative protection of these networks requires the Department to foster and maintain strong public-private partnerships, which improve planning, information sharing, and support response and restoration of the infrastructure when disruptions occur. While it is impossible to eliminate all vulnerabilities to communications infrastructure, the Department works with the private sector to make strategic improvements in security that minimize the likelihood of disruptions.

The Department's Communications Infrastructure Protection Mission

The Department's role in the communications infrastructure, as outlined in the Homeland Security Act of 2002, Homeland Security Presidential Directive (HSPD) 7, and Executive Order 12472, is to engage with Federal, state, local, tribal and private-sector partners to lead national-level efforts to enhance the overall protection of the communications infrastructure. As we have learned while protecting the Federal civilian government networks, cyber threats are unpredictable and evolving. Malicious actors continue to target the Nation's critical infrastructure, affecting our national and economic security.

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

We must continue designing a collaborative strategy that keeps our networks available, resilient, and reliable.

As the Sector Specific Agency under HSPD-7 for both the communications and information technology (IT) sectors, DHS, through the National Protection and Programs Directorate (NPPD)'s Office of Cybersecurity and Communications (CS&C), works closely with the communications and IT sector to ensure robust and resilient communications throughout the Nation. Within NPPD/CS&C, the National Communications System (NCS) leads this activity for the communications sector and the National Cyber Security Division (NCSD) works with the information technology sector. The National Cybersecurity and Communications Integration Center (NCCIC) houses the National Coordinating Center for Telecommunications (NCC), NCS's operational arm. The NCS leads the government-industry coordination critical in the planning, initiation, restoration, and reconstitution of national security/emergency preparedness (NS/EP) services and facilities. NPPD/CS&C's Office of Emergency Communications (OEC) supports and promotes the ability of emergency responders and government officials to continue to communicate in the event of natural disasters, acts of terrorism, or other man-made disasters. OEC works to ensure, accelerate, and attain interoperable and operable emergency communications nationwide. NPPD's collective efforts figure into a DHS-wide collaboration that extends to our partnerships with relevant Federal agencies, state and local governments, and the private sector. Together, these organizations are working to develop strategies to protect and mitigate threats to the communications infrastructure.

The security of the communications sector relies significantly on the IT sector. In recognition of this reliance, NCS and NCSD, as the Communications and IT Government Coordinating Council (GCC) chairs respectively, together with the relevant Sector Coordinating Councils (SCC), work closely on the policy and operational issues affecting both sectors. Each fall, the Communications and IT GCCs and SCCs hold the annual IT-Communications Sector Quad meeting, which brings together the government and private-sector stakeholders to discuss efforts and activities underway in each sector. Discussions cover efforts undertaken both independently and in partnership with each other and address issues affecting both sectors, including the cybersecurity of the two sectors.

Specific Programmatic Activities

The National Communications System

The NCS is an interagency system comprised of the telecommunications assets of 24 Federal agencies, each with significant operational, policy-related, regulatory, and enforcement responsibilities. The NCS coordinates telecommunications preparedness, response, and restoration activities across its 24 member agencies through the NCS Committee of Principals, which consists of senior government officials from each of the 24 member agencies, ensuring a diverse representation that includes the full range of Federal telecommunications assets. The NCS also coordinates responses with

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

stakeholders through the National Security Telecommunications Advisory Committee (NSTAC) and the NCC.

While cyber threats often necessitate unique assessment and mitigation strategies, protection of the communications infrastructure is also conducted in a holistic fashion, encompassing both physical and cyber threat mitigation strategies. Therefore, the Department leads national-level initiatives that are critical to addressing communications challenges associated with cyber attacks, deregulation, natural disasters, and terrorist attacks on our Nation. These efforts include risk assessment and management, technology enhancement, response coordination, and improvement of public-private bidirectional information sharing.

The NCS leads a number of risk assessment and management efforts, which improve the overall security of the communications infrastructure. For example, the NCS, through its partnership with the private sector, works to identify and mitigate vulnerabilities of those critical infrastructure interdependencies and dependencies. These partnerships facilitate the sharing of proprietary information in a secure environment on shared vulnerabilities in the communications sector, resulting in the ability to model and simulate wide-spread disruptions to the infrastructure. The Department employs mechanisms to ensure that sensitive and proprietary information is protected. The industry's willingness to share this information on a voluntary basis speaks to the strong trust between DHS and its private sector partners and the recognition that protection of our infrastructure is shared. Ultimately, these risk assessment and management efforts enable the sectors to incorporate, through coordination and collaboration, stringent security standards into those NS/EP technologies.

Under the National Infrastructure Protection Plan (NIPP), the NCS and the private sector jointly produce the Communications Sector Specific Plan (CSSP). The CSSP incorporates timely solutions and details a risk-management process that identifies and protects nationally critical architecture, ensures overall network reliability, maintains "always-on" services for critical customers, and quickly restores critical communications functions and services following a disruption. The development and implementation of the CSSP encourages public and private-sector partners to enhance the Nation's communications infrastructure protection framework. Sector partners will need to prioritize the actions set forth within this plan and coordinate their implementation accordingly.

NCS is working with its government and industry partners to mitigate cybersecurity threats to the communications infrastructure. For example, CSSP identifies specific risk management programs that mitigate cybersecurity threats, including the 2012 National Sector Risk Assessment (NSRA) and Supply Chain Working Group. In addition, NCS participated in cybersecurity testing and response capabilities during National Level Exercise 2011 Eagle Horizon and Cyber Storms II and III Exercises. NCS also led a cyber working group that evaluated how vulnerabilities impact the confidentiality and integrity of a network's data, as well as the availability of a network to meet the needs of its users. The working group focused on six broad categories of cyber risk across broadcasting, cable, satellite, wireless and wireline networks. The 2012 NSRA will

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

address cyber risks, as well as physical and human vulnerabilities, which may include supply-chain risk to the communications infrastructure.

National Security and Emergency Preparedness Communications

Incorporating security at the beginning of technology development or enhancement remains a priority for DHS with regard to NS/EP communications and cyber challenges. NCS is engaging in a number of initiatives to ensure security requirements are addressed throughout the acquisition lifecycle of all products and services. For example, through the development of its Next Generation Networks Priority Service Program, the NCS is working with the private sector to conduct in-depth cybersecurity analyses that identify security risks on the infrastructure that threaten NS/EP communications. A critical component of ensuring proper security is modeling and analysis. The NCS leads modeling, analysis, and technology assessments of current and future protocols, algorithms, network designs, and capabilities that will impact priority service communications in legacy and next-generation networks.

Playing a role in standards setting is also critical to ensuring that cybersecurity features are incorporated into the communications infrastructure. NCS participates in domestic and international standards-forming and -setting bodies to ensure that security considerations are appropriately addressed, including the International Telecommunications Union, the Internet Engineering Task Force and the Institute of Electronics and Electrical Engineers. These efforts lead to the development and implementation of national and international standards and ensure adoption of non-proprietary solutions for the United States' NS/EP communications industry-wide. International adoption of standards directly advances the United States' national and economic security interest by reducing the threats to our infrastructure and enabling our leadership and first responders to communicate during times of crisis.

Public-Private Partnerships

NCS has become a recognized means for the secure sharing of proprietary information among government and private-sector partners. For example, NCS formed the Network Security Information Exchanges (NSIE), a forum where government and industry share sensitive (proprietary) information. This information includes threats to operations, administration, maintenance, and provisioning of systems supporting the communications infrastructure in a trusted environment. The Federal Government membership has historically included representatives from the Intelligence Community and the Departments of Justice, Homeland Security, Defense, and Energy. As an all-voluntary forum, the group meets to identify intrusion activities, vulnerabilities that may lead to intrusion and exceed permission, significant malicious code, hackers, and other threats to the public network. This information is shared in real-time across government and private-sector partners through the US-CERT web portal.

Communications Information Sharing and Analysis Center

Information Sharing and Analysis Centers (ISACs) are an effective private-sector information-sharing and analysis mechanism. ISACs are sector-specific entities that advance physical and cyber critical infrastructure protection efforts by establishing and maintaining frameworks for operational interaction among members and external sector

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

partners. The Communications ISAC (COMM-ISAC) leverages the interagency and public-private capabilities of the NCC and supports the initiation, coordination, restoration, and reconstitution of NS/EP communications services or facilities under all conditions of crisis or emergency. As a consortium of over 56 private-sector partners, the COMM-ISAC provides the NCC with situational and operational information on a regular basis, as well as during a crisis, and provides information to NCS. NCS, in turn, shares information with the White House and other DHS components. This information exchange is vital for ensuring the protective posture of both the communications and IT sectors.

National Coordinating Center for Telecommunications

The NCC is the 24x7 operational arm of NCS and works closely with other coordinating bodies across Federal, state, and local governments, as well as the private sector. The NCC assists in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities. The NCC serves as the center for voluntary collaboration; information sharing; and vulnerability, threat and anomalies assessments to the communications infrastructure.

The President's National Security Technology Advisory Committee (NSTAC)

The Secretary of DHS serves as the Executive Agent for the NCS, which provides support to the President's NSTAC. The NSTAC is composed of up to 30 chief executives from industries like network service providers and telecommunications, information technology, finance, and aerospace companies. The NSTAC makes recommendations to the President on strategies and practices to secure vital telecommunications links through any event or crisis, as well as help the Government to maintain a reliable, secure, and resilient national communications infrastructure. Fulfillment of these responsibilities often take place across five key themes: strengthening national security, enhancing cybersecurity, maintaining the global communications infrastructure, assuring communications for disaster response, and addressing critical infrastructure interdependencies and dependencies.

National Cyber Security Division

NCSD is charged with securing the Nation's critical information infrastructure. To achieve its mission, NCSD works with public, private, and international partners to secure cyberspace and the Nation's cyber assets.

Communications Sector Supply Chain Threats

NCSD has partnered with both NCS and the communications sector to address Information and Communication Technology (ICT) supply-chain threats, which increasingly pose a risk to the ability of the Federal Government and critical infrastructure to engage in mission-essential functions. Due to the amount of communications infrastructure critical for public sector functions that is owned and operated by the private sector, the Supply Chain Risk Management (SCRM) program within NCSD, in coordination with NCS, is developing a partnership between government and industry to adequately address these supply-chain concerns and

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

collaboratively share relevant threat, vulnerability, and impact information with the CSCC. An interagency working group was formed to identify SCRM best practices, mitigation opportunities, and long-term planning to institutionalize effective models for SCRM across the sector. The group identified gaps in the Federal Government's understanding of telecommunications infrastructure, in both the Government's and private sector's understanding of the threat, and in the Government's access to an appropriate risk model to manage the supply chain. Through this evolving partnership, the NCSA is working to better identify and mitigate supply-chain security risks associated with sensitive elements of the telecommunications infrastructure.

The Information Technology Sector Specific Agency (IT SSA)

NCSA, as the IT-SSA, is the lead Government representative for the public-private partnership to secure national IT infrastructure. NCSA works with public and private sector partners to implement the IT Sector Specific Plan and risk management framework to assure the security and resiliency of the IT Sector. Additionally, NCSA facilitates cybersecurity sector-wide and cross-sector risk management across the U.S. critical infrastructure sectors through formal engagement; development of sector cybersecurity strategies; cyber infrastructure identification methodologies; and alignment of cybersecurity risk management approach with sector security strategy, risk assessment, and protective measures initiatives.

NCSA also leverages the sector partnership framework to work on cybersecurity issues that stretch across critical infrastructure sectors, including the communications sector, specifically through the Cross Sector Cyber Security Working Group (CSCSWG). The CSCSWG is a body with members drawn from each of the 18 critical infrastructure sectors, ensuring cross-sector collaboration on the cybersecurity issues facing all sectors.

Office of Emergency Communications

Nationwide Public Safety Broadband Network

Following the tragic events of September 11, 2001, members of the emergency response community – police officers, firefighters, emergency medical service (EMS) personnel – have worked with DHS to strengthen their emergency communications capabilities through enhanced coordination, planning, training, and new equipment. The creation of OEC was an important step toward improving the communications capabilities of those who are often the first to arrive at the scene of an incident—the Nation's emergency responders.

Recent developments in high-speed, wireless communications technology have presented an opportunity to provide public safety members with enhanced capabilities to share information and communicate during emergencies and day-to-day operations. Through the President's Wireless Innovation and Infrastructure Initiative (WIII), the Administration outlined its commitment to the development and deployment of the Nationwide Public Safety Broadband Network (NPSBN) for use by emergency responders in all parts of the country. This initiative supports a key recommendation from the National Commission on Terrorist Attacks Upon the United States, which called

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

for the establishment of a nationwide, interoperable public safety communications network to resolve the communications challenges faced by emergency responders seeking to rescue victims and restore order.

The prospects of having a nationwide interoperable broadband network took a major step forward when the “Middle Class Tax Relief and Job Creation Act of 2012,” was signed into law on February 22, 2012. Title VI of the new law, “Public Safety Communications and Electromagnetic Spectrum Auctions,” advances key components of the President’s WIII, including provisions to fund and govern the NPSBN. One of the most critical aspects of the law is the creation of a nationwide governance structure to oversee the network. The Administration believes that oversight is critical to ensuring that the NPSBN is a secure network that provides fully interoperable capabilities for all of our Nation’s first responders.

To ensure oversight and governance of the network, the new law establishes the First Responder Network Authority (FirstNet) within the Commerce Department’s National Telecommunications Information Administration (NTIA). Among its many responsibilities, FirstNet is directed to take “all actions” needed to ensure the construction, development, and deployment of the NSPBN, in consultation with Federal, state, local, and tribal public-safety entities. FirstNet is also required to ensure the safety and resiliency of the NPSBN, including protecting and monitoring against cyber attacks. As one of three Federal representatives on the FirstNet board, the Secretary of DHS will work with her Federal counterparts and the appointed members of the Board to ensure the successful deployment, governance, and operations of the NSPBN.

The deployment and security of this nationwide network will require significant collaboration among officials at all levels of government and the private sector, particularly with respect to leveraging existing partnerships and forging new ones to ensure the network is interoperable, secure, and state-of-the-art.

OEC is supporting the deployment of this network by continuing to work closely with the Departments of Commerce and Justice, as well as the Federal Communications Commission, on early implementation and planning efforts. In addition, OEC continues to work directly with Federal, state, local, and tribal stakeholders to provide policy guidance and planning assistance related to broadband emergency communications. Further, OEC has been tasked with continuing to coordinate with key DHS components and state and local public safety entities to ensure implementation of the envisioned nationwide network.

Under the strategy and policy direction of the One DHS Emergency Communications Committee, DHS has initiated a joint program management office to capture and implement Department-wide broadband requirements to develop a next generation tactical communications mobile platform for voice, data and video. This approach will align with commercial broadband technologies and public safety roadmaps to ensure cost efficiency and interoperability with Federal, state, local, and tribal partners.

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

These Federal coordination activities will be especially important in leveraging Federal expertise and assets in the areas of infrastructure protection and cybersecurity. Also, through its relationships with long-standing state and local collaboration groups, such as the SAFECOM Executive Committee/Emergency Response Council and the National Council of Statewide Interoperability Coordinators, OEC will continue to engage key public-safety leaders on a variety of issues regarding the development of the NPSBN, including security risks.

Securing the NPSBN

Once the NPSBN is deployed and operating, the network will increase communications interoperability, coordination, and response effectiveness by providing emergency responders with cutting-edge technologies and capabilities. However, we cannot overlook the security challenges that a new Internet Protocol (IP)-based communications network may also present. The NPSBN will interconnect many systems previously independent via IP networking, including public safety IT systems that transmit sensitive data, such as law-enforcement information and electronic medical records. While access to this data can help responders do their job more efficiently and effectively, it also presents new security risks, as this data could be highly valuable to cyber criminals and hackers.

That network must be secure and reliable so emergency responders can be assured that sensitive information is protected and accurate. Without careful planning on the front end, the NPSBN may find itself vulnerable to cyber attacks. As such, DHS has begun to examine potential security issues to the NPSBN and is well-positioned to assist FirstNet in building security into the foundation of the network. OEC, for example, is working with several stakeholder groups, including the National Public Safety Telecommunications Council and their established working groups, to discuss security issues for the NPSBN and to develop requirements. We will also leverage NCSD's work in the areas of standards and best practices from the cybersecurity community.

Together, OEC, NCSD, and NCS have started a risk assessment of the NPSBN. Since the Middle Class Tax Relief and Job Creation Act of 2012 was enacted, OEC has offered NTIA this continued assistance. OEC will coordinate with the necessary partners to conduct the assessment and will leverage NCSD's proven experience in cyber risk assessment methodologies. NCS will also provide input to the process based on past experience with risk assessments for the Communications Sector. The risk assessment will evaluate levels of risk in NPSBN physical infrastructure, data stored or transmitted on the network, and operational control systems. It will also help define, quantify, and prioritize risks. OEC will leverage the work done in this area by other partners, including the National Institute of Standards and Technology Public Safety Research Center. The risk assessment is expected to establish a process for managing cyber risks to the NPSBN, based on real-world experience and knowledge, which can be repeated as needed during the development and deployment of the NPSBN. DHS expects this to be the first of many ways in which the Department can work with and on behalf of FirstNet.

FOR OFFICIAL USE ONLY/PRE-DECISIONAL

Securing the NPSBN requires a holistic approach, with equal emphasis on protecting confidentiality, integrity, and availability. It also requires a collective effort from public safety, network managers, and industry partners to ensure that cybersecurity is built into the NPSBN from the bottom up. The work that public safety agencies, Federal partners, and industry are doing to ensure effective and secure network operations is a significant start, and DHS looks forward to continued partnerships with government and private-sector stakeholders to build a secure communications network for our Nation's first responders.

Thank you again for this opportunity to testify. I am pleased to answer your questions.