Statement for the Record
of
Gregory Schaffer
Assistant Secretary
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 Emergency Communications, Preparedness, and Response

July 27, 2010

Introduction

Chairwoman Richardson, Ranking Member Rogers, and distinguished Members of the Subcommittee, it is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) emergency communications mission. Today I will outline DHS's responsibilities in emergency communications. I will also discuss our position on the development and deployment of a nationwide public safety broadband network including the allocation of the Upper 700 MHz Band D Block radio spectrum. Finally, I will outline the steps that DHS, in coordination with the Federal Communications Commission (FCC) and other federal departments and agencies, has taken and plans to take to ensure that our nation's emergency responders have the ability to communicate as needed, on demand, and as authorized at all levels of government and across all disciplines.

The nation is at a critical juncture regarding the future of emergency communications. We have an opportunity to change the trajectory of how the United States responds to emergency events. Today, the needs of public safety users are being met by Land Mobile Radio (LMR) technologies, which are used across the nation by federal, state, local, and tribal governments to provide the mission-critical voice capabilities used every day by firefighters, law enforcement officers, emergency medical technicians, and other first responders to protect and save lives. In a broadband world in which voice, video, and data are available to every smartphone user, voice communications—while essential—are no longer sufficient to meet the needs of emergency responders. Public Safety also needs the data capabilities and efficiencies that newer technologies can provide.

The planned deployment of new fourth generation, or 4G, mobile technologies by many commercial carriers over the next several years presents a historic window of opportunity to secure a range of high-speed, cutting-edge, inherently interoperable capabilities for our nation's public safety and emergency response community. These new technologies can be leveraged to augment the existing LMR solutions that the public safety community currently uses to perform its vital mission: delivering a robust, operable, and interoperable nationwide public safety network. This improved network would support rural jurisdictions and urban areas alike, ensuring that all emergency responders have access to the new capabilities. If employed effectively, it will facilitate the development of new technologies tailored to public safety which could mean faster response times for ambulances and fire engines, as traffic-aware mapping systems guide responders around obstructions and along obscure roads and side streets, avoiding congested areas. Real-time video analysis could improve situational awareness and reduce risks to civilians. High-speed imaging transmissions could enhance the effectiveness of emergency medical treatment in remote locations, saving more lives. The possibilities, not unlike the demand for and use of applications on smartphones, for new life saving solutions and inventions are unlimited.

We support the vision of a national public safety broadband network, which leverages commercial technologies and applications, to meet public safety and emergency response requirements. Among the capabilities public safety needs are:

1. An infrastructure built to handle natural hazards
2. Nationwide interoperable coverage for all public safety agencies
3. Public safety-grade voice capability
4. Robust data services
5. Public Switched Telephone Network access
6. Satellite services

These services raise complex issues, but we are committed to ensuring strong capabilities for vital public safety communications.

Overview of DHS Emergency Communications Responsibilities

Within the Office of Cybersecurity and Communications, I manage two organizations that focus on different but converging areas of telecommunications: the Office of Emergency Communications (OEC) and the National Communications System (NCS). OEC was established as part of the congressional response to the communications challenges faced during the September 11, 2001 terrorist attacks and Hurricane Katrina in 2005. Created by Congress in 2006, OEC coordinates policy and assists in the development and implementation of interoperable and operable emergency communications capabilities for emergency responders at all levels of government—federal, state, local, tribal, and territorial. OEC provides more than

100 technical assistance visits to state and local partners each year and coordinates federal interagency emergency communications activities across 14 partner agencies through the Emergency Communications Preparedness Center, and across all levels of government through the SAFECOM Executive Committee and Emergency Response Council. OEC also led the development of the National Emergency Communications Plan (NECP).

The NCS, transferred from the Department of Defense to DHS in 2003, was created by executive order to support the telecommunications functions of the Executive Office of the President and all federal departments and agencies for Continuity of Government, Enduring Constitutional Government, and Continuity of Operations. The NCS is an interagency system comprised of the telecommunications assets of 24 federal departments and agencies, each with significant operational, policy, 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 across the NCS that includes the full range of federal telecommunications assets. The NCS developed, manages, and administers priority communications services that take advantage of existing capabilities provided by the privately owned public switched network (PSN), yielding a cost-effective emergency communications solution for government and critical infrastructure emergency responders.

If the PSN is damaged, degraded or congested during times of emergency, crisis or war, the NCS priority services allow senior federal officials and first responders to complete their calls. These priority services are maintained in a constant state of readiness through the NCS's unique public/private partnership with the PSN providers. The NCS also administers an FCC mandate that prioritizes restoration of critical national security and emergency preparedness circuits if they are damaged or destroyed during disasters or emergencies. Under the National Response Framework, the NCS is the lead agency responsible for executing Emergency Support Function #2 Communications. To ensure that effective and reliable communications exist to provide Continuity of Government, Enduring Constitutional Government, and Continuity of Operations, the NCS identified the minimum continuity communications requirements for all federal departments and agencies, and tests the operational readiness of those capabilities every month.

Both the OEC and the NCS are critical to shaping national policy, improving technological capabilities, and securing federal government support for a nationwide public safety broadband network. They work across DHS, federal departments and agencies, multiple levels of government, and private industry to improve communications capabilities and achieve their mission requirements.

In July 2008, OEC—working closely with our partners from all levels of government and the private sector—published the first National Emergency Communications Plan (NECP). The NECP established a clear operational vision for our nation's emergency communications efforts —that emergency responders can communicate as needed, on demand, and as authorized, at all levels of government and across all disciplines. This vision is not technology-specific but encompasses all the wide range of different means and methods that emergency responders use to communicate. The NECP established three measurable goals, the first of which we are currently in the process of evaluating:

- **Goal 1—**By 2010, 90 percent of all high-risk urban areas designated within the Urban Areas Security Initiative (UASI) are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.
- **Goal 2—**By 2011, 75 percent of non-UASI jurisdictions are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.
- **Goal 3—**By 2013, 75 percent of all jurisdictions are able to demonstrate response-level emergency communications within three hours, in the event of a significant incident as outlined in national planning scenarios.

This month we held 10 evaluations of Goal 1 progress. By the end of October of this year, we will have evaluated the communications capabilities of the nation's largest urban areas. Next year, we will expand upon this effort and evaluate Goal 2, coordinating with states to collect information at the county level and providing DHS with detailed performance and capability data from more than 3,000 local jurisdictions.

Through OEC, DHS has placed heavy emphasis on communications capacity building at the state and local level. At the center of this effort has been support for the development of extensive governance structures—including strategic plans, governance bodies, and the identification of statewide leadership—in order to strategically guide emergency communications investments in states and localities. Interoperability is not just about enabling technologies -- it is as much about the people and processes necessary to use technology in an interoperable way.

The investments we have made over the past several years in governance can be fully leveraged as new broadband technologies are integrated into the suite of solutions that will be used by the public safety community in the future. Today each of the nation's 56 states and territories has Statewide Communications Interoperability Plans and Statewide Interoperability Governing Bodies to guide their efforts to improve emergency communications capabilities across their states. In addition, 44 states have hired full-time Statewide Interoperability Coordinators to lead the effort to build interoperable emergency communications networks. These planning structures, people and processes, are the crucial building blocks necessary to successfully

integrate broadband communications networks into the overarching emergency communications enterprise. In many ways, the emergency response community is poised to take this next step.

These organizational efforts are complemented by the priority services programs managed by the NCS. The nation's telecommunications providers are transitioning from the current circuit switched technology to next generation network (NGN) Internet protocol (IP) packet-switched technology. The NCS is working closely with private industry, national, and international standards bodies to ensure that current priority service capabilities continue. The NCS' NGN program is intended to ensure that all national security and emergency preparedness users continue to have priority service capabilities in the next-generation network environment. These capabilities, and NCS's expertise, provide vital support to public safety communications as the nation migrates towards an IP-based communications environment.

Dual Path Model

As broadband communications capabilities are layered into the emergency communications enterprise, it is essential that we leverage the strategies, policy, governance structures, and coordination groups that support current emergency communications capabilities to address the challenges and opportunities of the broadband world. We are not starting from scratch, and we cannot forget the importance of continuing to support and improve current day-to-day mission critical communications capabilities. Based on everything we know today about both the state of the technology and the resources of the community, we believe that it is unlikely that public safety would transition away from LMR in fewer than 10 years. As the first broadband systems are built, they will primarily come in the form of broadband wireless cards for laptops, not ruggedized public safety handsets that handle both data and voice transmissions. While a single unified broadband solution for both data transmission and mission critical voice should ultimately be possible, only with future refinement of standards, significant research and development, and rigorous testing and evaluation will we be able to begin moving forward with the transition from mission-critical voice communications to broadband networks.

As we concentrate and unify our efforts on building broadband communications capabilities, we will continue to partner with public safety to ensure continued, robust interoperability alongside full broadband implementation. Our goal is to make certain that all emergency responders have the capabilities needed to perform their essential missions, with respect to both today's communications infrastructure and emerging broadband technologies.

Broadband Network Policy Requirements

As DHS evaluates any potential plan to develop and deploy a nationwide public safety broadband network, we are focused on a number of guiding principles. First and foremost, interoperability must be built into any network architecture proposal from the outset. We must use lessons learned from the creation of the LMR environment and avoid developing systems that are unable to interoperate with each other without substantial investment in expensive add-on components.

Second, coverage in both urban and rural areas is mission-essential. Emergency responders across the entire range of response official—from metropolitan police departments to rural county volunteer fire departments—must benefit from broadband communications capabilities to meet their mission requirements. This network must be able to address earthquakes in San Francisco as well as wild fires in Montana. It needs to provide coverage for potential terrorist events in New York City and hurricanes in rural Louisiana. This effort is about connecting everyone, no matter where in the United States they live.

Third, the solution must allow public safety devices to heavily leverage commercial technology. Within the current LMR environment, public safety handset costs can range from hundreds to several thousands of dollars per unit, largely because they are not able to leverage the economies of scale from which commercial customers benefit. The same generally holds true for infrastructure components—towers, base stations, switching equipment, antennae, and backhaul facilities. If public safety and commercial providers can leverage common infrastructure, chipsets, and base station technologies which also meet public safety requirements, both sides will benefit.

Finally, any solution must provide a path for the network to evolve and grow, progressively adding greater capability and providing better mission support.

The release of the FCC's National Broadband Plan (NBP) has focused much needed attention on developing a nationwide public safety broadband network. While reactions have been strong both for and against elements of the plan, DHS believes that the increased attention to this challenge, and ensuring transparency in meeting it, will result in stronger solutions. The NBP's key public safety recommendations are far-reaching and the Administration is currently examining the NBP as part of the National Science and Technology Council's sub-committee on broadband. DHS is working closely with the Administration on the Public Safety portions of the plan.

The Administration strongly supports building a national public safety broadband network capable of meeting the mission requirements of public safety. Moreover, the Administration is committed to a dedicated funding stream to help fund the network using revenues derived from spectrum initiatives.

The Administration recently provided the opportunity for funding a portion of the nationwide public safety broadband network when the Department of Commerce reopened the second round of the Broadband Technology Opportunities Program (BTOP) to allow 21 jurisdictions to compete with other applications for federal grant funding. If a public safety applicant is successful, they may use those funds to begin building out systems that make use of public safety broadband spectrum. We support the FCC's decision to grant waivers to these 21 jurisdictions for conditional use of currently allocated spectrum to promote the development of technological solutions, processes, and procedures that can inform the deployment of other jurisdictions throughout the United States. We are hopeful that these applicants will submit competitive, well thought out applications. Successful public safety applicants could help lead the way and accelerate the development and deployment of broadband communications capabilities across the United States. At the same time, we note that it is critically important that these jurisdictions build to a single consistent standard so that the resulting system of systems is both operable and interoperable.

The Department of Commerce is also sponsoring a significant initiative—the Public Safety Broadband Demonstration Network—at its Boulder, Colorado labs, where federal agencies, public safety, and industry will come together to promote public safety broadband technologies and evaluate equipment. This initiative will help ensure that objective data can be provided to public safety on the capabilities and limitations of broadband devices as they become available. Earlier this month I visited the Boulder labs as part of DHS's ongoing efforts to ensure that public safety's technical questions and needs are being addressed. Among other efforts, DHS is facilitating direct public safety community participation in the evaluation process and looks forward to continuing to partner with the Department of Commerce to ensure that emergency responders can participate in these efforts.

The D Block

At the Department, our efforts are focused on ensuring that public safety has the capabilities to communicate as needed, on demand, and as authorized at all levels of government and across all disciplines. The arguments for and against reallocation of the D Block are extremely complex, and we believe that any proposal must meet the needs of public safety and adhere to the guiding principles I laid out earlier. Under the FCC's proposal, public safety communications would transition into a commercial environment characterized by increased infrastructure to maximize spectrum reuse and the utilization of commercial chipsets and base station technology to achieve significant cost and capability advantages for public safety users and the nation. We believe that the FCC's proposal has merit, with a number of significant caveats.

First, the FCC's proposal relies on development of a new generation of technical capabilities and additional legal authorities, which are intended to allow public safety to roam onto commercial spectrum with priority access in emergency events. Both the technical and legal frameworks for this type of plan must be evaluated, and capacity and capability outcomes understood, before any decision can be made regarding the spectrum requirements for public safety.

Second, the FCC's plan will necessitate sufficient funding to build out the infrastructure required for the network. Effective network operations require that sufficient cell sites and base stations be built out and that the network be hardened as appropriate. One significant advantage of the FCC's plan is that network costs are expected to be significantly less than other alternatives, and costs are of course an important factor for public safety..

Third, the FCC expects that commercial networks can ultimately be enabled to handle not only mission-enhancing public safety data communications traffic but eventually, mission-critical public safety voice traffic as well. While the use of Long Term Evolution wireless broadband technology as a replacement for existing public safety voice-traffic systems is years away, it is essential that significant efforts be undertaken now to solve the following critical technical challenges associated with public safety use of commercial networks:

1. The networks and associated equipment must be able to operate in a one-to-many mode, as LMR systems do today, in addition to the one-to-one mode of typical commercial cellular phone systems.
2. The networks and associated equipment must be able to operate peer-to-peer (or handset-to-handset) in the event of network outages;
3. The networks must be able to provide clear understandable voice communications in high-noise environments like burning buildings, and with minimal voice delay; and
4. The networks must be able to penetrate to and from the interior of large buildings without significant degradation of capability.

The Path Forward

To move forward, working in close partnership with the public safety and emergency response community, and with support from the FCC, the Administration, through the Department of Homeland Security and the Department of Justice is establishing a joint task force on public safety interoperability to better understand and identify public safety requirements, test assumptions and approaches associated with meeting those requirements, recommend technical, policy, process, and governance solutions, and coordinate with the FCC. This task force will allow personnel from several of the departments and agencies with major interoperability competencies to work in partnership with the public safety community.

The Administration also plans to convene a forum this fall to discuss funding, spectrum requirements, technology issues, and governance models necessary to support the development of a next generation network for public safety communications.

DHS Support

DHS is committed to supporting public safety and pursuing a dual path strategy that steadily improves mission-critical voice communications capabilities while investing in the deployment of a nationwide public safety broadband network. We will continue to provide technical assistance and governance support, share best practices and lessons learned, and provide venues for coordination for our nation's emergency responders as they maintain and improve their day-to-day mission-critical communications networks, procedures, and protocols.

We will support the 21 waiver jurisdictions as they begin their efforts to deploy the nation's first public safety broadband systems in 700 MHz public safety spectrum. We will work with these jurisdictions to ensure that their efforts create an interoperable system of systems that allows users from all jurisdictions to converge and operate seamlessly in the event of an incident of national significance. We will leverage the best practices and lessons learned from these efforts to encourage their integration into broadband communications capabilities.

Within the next year, we will release a revised version of the NECP, which will lay out the policy and strategic direction for integration of public safety communications across all technology platforms and more explicitly integrate the dual path model. We will also apply our IP packet prioritization and standards expertise to the challenges facing the public safety community.

We look forward to working with other federal departments and agencies and Congress to explore additional opportunities for federal partnerships with a new nationwide public safety broadband network.

Conclusion

We must seize the opportunity to build a nationwide public safety broadband network that will provide cutting-edge capabilities to our first responders. We will aggressively work to support public safety agencies as they integrate broadband data capabilities into their emergency communications systems, protocols, and governance structures. This is a once-in-a-generation opportunity, and we must get it right.

Thank you for this opportunity to testify, and I would be happy to answer your questions.