

**Written Statement
of
Michael L. Alagna
Director of Homeland Security Strategic Initiatives and Policy
Motorola, Inc.
Before the
Homeland Security Subcommittee on Emergency Communications,
Preparedness, and Response
United States House of Representatives
July 15, 2008**

Good morning Chairman Cuellar, Ranking Member Dent and other distinguished Members of The Subcommittee. I am Michael Alagna, Director of Homeland Security Strategic Initiatives at Motorola. I appreciate the opportunity to provide testimony to this Subcommittee regarding industry perspectives on the development of the National Emergency Communications Plan.

I would like to begin by commending Congress, and, in particular, this Committee, for its leadership to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and ensure, accelerate, and attain interoperable emergency communications nationwide.

By way of background, at Motorola, I am focused on homeland security, national security and emergency preparedness initiatives. I presently serve on the Industry Executive Subcommittee for the National Security Telecommunications Advisory Committee (NSTAC). I co-chaired the NSTAC Report on Emergency Communications and Interoperability, published in January 2007. The NSTAC provides industry-based analyses and recommendations on policy and enhancements to national security and emergency preparedness (NS/EP) communications. Another of my roles is with the Department of Homeland Security's Critical Infrastructure Partnership Advisory Council (CIPAC); I am Motorola's representative to the Communications Sector Coordinating Council (C-SCC) and was just elected vice chair.

First let me say that Motorola applauds Congressional action with the 21st Century Emergency Communications Act of 2006 that established in the Department an Office of Emergency Communications to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters; and ensure, accelerate, and attain interoperable emergency communications nationwide. As a result, Congress directed the DHS' Office of Emergency Communications (OEC) to develop a plan to:

- Identify the capabilities needed by emergency responders to ensure the availability and interoperability of communications during emergencies, as well as obstacles to the deployment of interoperable communications systems

- Recommend both short- and long-term solutions for ensuring interoperability and continuity of communications for emergency responders, including recommendations for improving coordination among Federal, State, local, and tribal governments
- Provide goals and timeframes for the deployment of interoperable emergency communications systems and recommend measures that emergency response providers should employ to ensure the continued operation of communications infrastructure
- Set dates and provide benchmarks by which State, local, and tribal governments and Federal agencies expect to achieve a baseline level of national interoperable communications
- Guide the coordination of existing Federal emergency communications programs.

Furthermore, Motorola and industry broadly supported the Office of Emergency Communications approach of stakeholder involvement as the single most important element in the NECP development process. Congress directed the OEC to develop the NECP in cooperation with state, local, and tribal governments; federal departments and agencies; emergency response providers; and the private sector. Industry involvement was coordinated through the Critical Infrastructure Partnership Advisory Council (CIPAC), which included representatives from the Communications Sector Coordinating Council. OEC also coordinated with industry representatives from the National Security Telecommunications Advisory Committee (NSTAC) Emergency Communications and Interoperability Task Force.

As a key first phase in the development process, OEC drew heavily from a foundation of emergency communications documentation and initiatives. These source documents were key drivers for the NECP's assessment of the current state-of-emergency communications and also helped shape the Plan's strategic goals, objectives, and initiatives. For example, the NSTAC report on Emergency Communications and Interoperability anticipated incorporating critical elements into the NECP, such as: large scale state and regional shared public safety communications networks and supporting federal grants; yearly benchmarks for achieving defined interoperability objectives; nationwide outreach to support emergency response communications; consolidation of federal operations centers to increase coordination and situational awareness; and identification of specific private sector emergency communications and interoperability support roles. The NSTAC report also suggested the establishment and incorporation of the following capability objectives into the National Emergency Communications Plan (NECP): support for a significantly expanded user base; full leveraging of network assets; internet protocol based interoperability; assured access for key users through priority schemes or dedicated spectrum; national scope with common procedures and interoperable technologies; deployable elements to supplement and bolster operability and interoperability; resilient and disruption-tolerant communications networks;

network-centric principles benefiting emergency communications; and enhanced communications features.

During the final phases of Plan development, OEC conducted outreach to review the document with industry. OEC once again engaged the Office of Infrastructure Protection's CIPAC to review the NECP with the communications and emergency services sectors. While a majority of the plan is inherently governmental, industry strongly supported the primary elements of the NECP, namely:

- Enhance resiliency and redundancy for public safety systems, including back-up solutions, to ensure communications are maintained and/or restored following catastrophic incidents.
- Ensuring and improving mission-critical voice, data, and video communications interoperability for emergency response providers and relevant government officials
- Improving coordination of emergency communications efforts between federal and state, local, and tribal emergency response providers
- Positioning the public safety community to take advantage of emerging technologies and solutions for emergency communications

The following comments reflect industry perspectives gained during development of the NECP and reviews conducted during the CIPAC process.

A. Enhance Resiliency and Redundancy for Public Safety Systems, Including Back-Up Solutions, to Ensure Communications are Maintained and/or Restored Following Catastrophic Incidents.

Emergency communications among those responding to a natural disaster, terrorist attack, or other large-scale emergency are critical to an effective response. Emergency communications systems need to be designed and constructed to withstand worst-case scenarios expected in a region. First responders have called this the need for system "operability," meaning that systems must first survive and function. Systems must maintain communications capabilities during all phases of a disaster or event. Emergency responders need solutions to account for and mitigate the potential impact of communications infrastructure damage, including the destruction of telephone lines, public safety networks, towers, and sustained loss of power.

Mission critical, resilient and disruption-tolerant communications networks allow emergency responders and relevant government officials to have assured access to communications channels to support their ability to coordinate response and recovery throughout all stages of emergencies. Recommendations suggested that users define, specify and procure resilient and disruption-tolerant communications networks including priority access and restoration services, emergency power back-up, site hardening and redundancy, fault and network performance management capabilities.

Industry also recommended the development of an emergency communications “operability” program, (much like SAFECOM has done for interoperability) to include functionality, security, redundancy and performance. The Office Emergency Communications (OEC) should establish a comprehensive definition of operability in partnership with the emergency response community and support the development of guidance, tools and templates to ensure levels of operability and related research, development, testing, evaluation and standards. The OEC should consider expanding the National Baseline Survey to include a mechanism for determining and measuring the state of operable communications nation-wide and should gather information to guide and measure the effectiveness of future communications operability improvement efforts that local, tribal, state, and Federal emergency response organizations execute. Incentives for organizations to improve operability should also be examined.

B. Ensuring and Improving Mission-Critical Voice, Data, and Video Communications Interoperability for Emergency Response Providers and Relevant Government Officials

In addition to emergency communications system operability concerns, a further major barrier to effective responder communications is the widespread lack of interoperability which impedes communications and critical information sharing across dissimilar emergency responder systems. There are positive steps being taken by leaders within the public safety community, key federal programs, the Congress and industry to significantly accelerate the current environment and move the state of interoperability forward.

Interoperability is enabled by Project 25 (or P25), a full suite of standards that provides the basis for interoperable digital radio voice and moderate speed data communications among multiple public safety users, departments and agencies. The Project 25 standards were developed by the public safety users and are published by the Telecommunications Industry Association. Both DHS and public safety users support Project 25 because it is an open architecture solution and enhances the transition to digital radio technology.

P25 improves spectrum efficiency, enables more competitive procurements, and displaces vendor proprietary systems that can not interoperate. P25 has been endorsed by virtually all public safety organizations and has received additional strong support at the federal level, including from DOD, DOJ, and FCC. Additionally, most states have either built P25 systems, are in the process of doing so, or have plans to do so.

This committee’s strong leadership in supporting P25 has been very valuable in assuring that DHS grant programs continue to promote this important standard as federal funds are directed toward improving interoperability. Industry supports the NECP’s promotion of a standards based approach to interoperability and other emergency communications issues.

Increasingly, the campaign for interoperability has expanded beyond voice communications to encompass data and video interoperability that will necessitate the expansion of standards efforts to encompass data and video applications to improve

communication between State and local governments and between neighboring local jurisdictions.

Additional recommendations for solutions to improve interoperability capacities of law enforcement, firefighters, and other emergency responders to respond to and manage incidents included suggestions such as agencies struggling with deploying interoperable emergency communications capabilities should consider joining regional and statewide initiatives; state and federal grants should support multi-agency cooperation; neighboring agencies should collaborate in planning and acquiring communications systems. The concept of shared system architecture for emergency responders, especially in a statewide geography brings state agencies and local county and municipal first responders together onto a common network for shared voice and data services. Recent trends towards regional, multi-jurisdictional and multi-disciplinary approaches can meet the needs of city, county and local users while improving day-to-day mission effectiveness and incident response interoperability when needed.

To improve the governance issues associated with multi-jurisdictional communications, industry recommended working with the National Governors Association (NGA) as a critical link in overcoming the obstacles to interoperability. This organization can provide the leadership necessary to develop and institutionalize a governance structure that fosters collaborative planning among local, state, and federal agencies, that insures multi-agency coordination of public safety communications.

C. Improving Coordination of Emergency Communications Efforts between Federal and State, Local, and Tribal Emergency Response Providers

Industry supports better planning for how the mission critical, interoperable communications systems of federal civilian agencies and U.S. military will interoperate with state and local responders during events of national significance. While disaster preparedness and response to most incidents remains a State and local responsibility, recent events demonstrated the need for greater integration and synchronization of preparedness efforts among a dynamically expanding user base beyond traditional first responders (e.g., military, National Guard, critical infrastructure providers, and public health system users).

Better planning for how federal civilian agencies, the U.S. military, international partners and state and local responders interoperate along border regions poses many unique challenges. Local law enforcement agencies in border communities are expected to communicate and work in conjunction with not just local, state and federal agencies but with Canada and Mexico. The improving America's Security Act of 2007 establishes future demonstration projects along our international borders will improve collaboration and help identify solutions to interoperable communications requirements.

Industry also plays a critical role for improving coordination of emergency communications efforts. While the Federal Government recognizes the significance of the communications infrastructure in providing essential services during and after a natural disaster or terrorist attack, lessons learned demonstrate that vital communications

restoration efforts were stalled with infrastructure providers having difficulty gaining access to repair essential infrastructure. Currently, there is no standard Government policy for private sector use for access and perimeter control issues, this is especially important given that perimeter access policies, in general are subject to State and local regulation and enforcement.

D. Positioning the Public Safety Community to take Advantage of Emerging Technologies and Solutions for Emergency Communications

Future-focused technologies are rapidly increasing the range of features, devices, applications and available bandwidth that support incident response and recovery. New communications capabilities, including greater access to data and new services, will support emergency communications functions in critical ways, enabling emergency responders, for example, to obtain real-time access to voice, data, and video necessary for the most effective completion of their missions. Solutions must be found that address emergency communications functional requirements, within these new applications, especially for security and availability.

With specific mission critical enhancements to commercial internet and mobile wireless technologies, and advances in innovative gateway technologies for bridging land mobile radio networks to Internet Protocol (IP) networks, a new class of interoperable voice, data and multimedia service can be envisioned with mobility across any and all available access networks. Multiband and multimode subscriber devices will improve wireless access across these available networks.

Solutions for emergency communications capabilities need to incorporate the range of features (e.g., voice, data, multimedia, push-to-talk) that best support the needs of emergency communications users. Continually evolving emergency responder requirements and the advent of new technologies will lead to necessary updates and revisions to interfaces and subsequent standards.

Summary

The NECP lays out actionable steps to be taken by leaders within the emergency response community, key federal programs, the Congress and industry to significantly accelerate the current environment and move the state of emergency communications forward. The NECP identifies private sector support to communications during emergencies and recovery efforts and provides direction for private sector involvement in standards development, advanced communications technologies, and services development and deployment. Continued involvement of representatives of the private sector as advisors to governmental groups developing their emergency communications requirements is critical. In order for the NECP to be successful, the emergency response community of Federal, State, local, tribal, and private sector must work together and support each other to achieve nationwide operability, interoperability, and continuity of emergency communications.

Summary

Michael L. Alagna, Motorola, Director of Homeland Security, Strategic Initiatives & Policy, 1455 Pennsylvania Avenue, 9th Floor, Washington, DC 20004, 410.750.0572 tel, 410.409.3447 mobile, 202.842.3578 fax, mike.alagna@motorola.com

Background

Industry broadly supported the Office of Emergency Communications approach of stakeholder involvement as the single most important element in the NECP development process. Industry involvement was coordinated through the Critical Infrastructure Partnership Advisory Council (CIPAC), which included representatives from the Communications Sector Coordinating Council. OEC also coordinated with industry representatives from the National Security Telecommunications Advisory Committee (NSTAC) Emergency Communications and Interoperability Task Force. As a key first phase in the development process, OEC drew heavily from a foundation of emergency communications documentation and initiatives. For example, the NSTAC report on Emergency Communications and Interoperability anticipated incorporating critical elements and capability objectives into the National Emergency Communications Plan (NECP). During the final phases of Plan development, OEC conducted outreach to review the document with industry. While a majority of the plan is inherently governmental, industry strongly supported the primary elements of the NECP:

Enhance Resiliency and Redundancy for Public Safety Systems

Emergency communications systems need to be designed and constructed to withstand worst-case scenarios expected in a region. Emergency responders need solutions to account for and mitigate the potential impact of communications infrastructure damage. Industry also recommended the development of an emergency communications "operability" program, to include functionality, security, redundancy and performance. The (OEC) could consider expanding the National Baseline Survey to include a mechanism for determining and measuring the state of operable communications nation-wide and could gather information to guide and measure the effectiveness of future communications operability improvement efforts that local, tribal, state, and Federal emergency response organizations execute. Incentives for organizations to improve operability could also be examined.

Ensuring and Improving Mission-Critical Voice, Data, and Video Communications Interoperability

In addition to emergency communications system operability concerns, a further major barrier to effective responder communications is the widespread lack of interoperability which impedes communications and critical information sharing across dissimilar emergency responder systems. There are positive steps being taken by leaders within the public safety community, key federal programs, the Congress and industry to significantly accelerate the current environment and move the state of interoperability forward. Interoperability is enabled by Project 25 (or P25), a full suite of standards that provides the basis for interoperable digital radio voice and data communications. This committee's strong leadership in supporting P25 has been very valuable in assuring that DHS grant programs continue to promote this important standard as federal funds are directed toward improving interoperability. Industry supports the NECP's promotion of a standards based approach to interoperability and other emergency communications issues.

Improving Coordination of Emergency Communications between Federal and State, Local, and Tribal Emergency Responders

Better planning for how the mission critical, interoperable communications systems of federal civilian agencies and U.S. military will interoperate with state and local responders during events of national significance is required. While disaster preparedness and response to most incidents remains a State and local responsibility, recent events demonstrated the need for greater integration and synchronization of preparedness efforts among a dynamically expanding user base beyond traditional first responders (e.g., military, National Guard, critical infrastructure providers, and public health system users). Also coordination along border regions poses many unique challenges as federal civilian agencies, the U.S. military, international partners and state and local responders must interoperate. Local law enforcement agencies in border communities are expected to communicate and work in conjunction with not just local, state and federal agencies but with Canada and Mexico. The improving America's Security Act of 2007 establishes future demonstration projects along our international borders will improve collaboration and help identify solutions to interoperable communications requirements.

Positioning the Public Safety Community to take Advantage of Emerging Technologies and Solutions

New communications capabilities, including greater access to data and new services, will support emergency communications functions in critical ways, enabling emergency responders, for example, to obtain real-time access to voice, data, and video necessary for the most effective completion of their missions. Solutions must be found that address mission critical emergency communications functional requirements, within these new applications, especially for security and availability. Solutions for emergency communications capabilities need to incorporate the range of features (e.g., voice, data, multimedia, push-to-talk) that best support the needs of emergency communications users. Continually evolving emergency responder requirements and the advent of new technologies will lead to necessary updates and revisions to interfaces and subsequent standards.

Summary

The NECP lays out actionable steps to being taken by leaders within the emergency response community, key federal programs, the Congress and industry to significantly accelerate the current environment and move the state of emergency communications forward. The NECP identifies private sector support to communications during emergencies and recovery efforts and provides direction for private sector involvement in standards development, advanced communications technologies, and services development and deployment. In order for the NECP to be successful, the emergency response community of Federal, State, local, tribal, and private sector must work together and support each other to achieve nationwide operability, interoperability, and continuity of emergency communications.