Written Testimony of
Linda K. Moore
Specialist in Telecommunications Policy
Congressional Research Service

"Ensuring Coordination and Cooperation: A Review of Emergency Communications Offices Within the Department of Homeland Security"

Before the
Committee on Homeland Security
Subcommittee on Emergency Preparedness, Response, and Communications
U.S. House of Representatives
November 17, 2011

Chairman Bilirakis, Ranking Member Richardson, and members of the Subcommittee, I am honored to be testifying before you today on behalf of the Congressional Research Service. My name is Linda Moore and for the past ten years my responsibilities at CRS have included providing Congress with information and analysis regarding emergency communications, including 911, the Emergency Alert System, and radio communications for first responders. My testimony today provides an overview of key provisions in legislation passed since September 11, 2001 that have addressed radio communications interoperability and operability for public safety agencies. This testimony is based on CRS reports and memoranda written during the period 2002 through 2011.

Prior to September 11, 2001, meeting the communications needs of first responders was primarily a local or state responsibility. The federal government provided some assistance and support. For example, in 1997, Congress instructed the Federal Communications Commission (FCC) to assign additional radio frequency spectrum capacity for public safety, based on recommendations by the federally sponsored Public Safety Wireless Advisory Committee.

The Homeland Security Act of 2002

The Homeland Security Act of 2002 (P.L. 107-296) included some requirements that provided the basis for federal leadership to address public safety communications needs. Title I of the Homeland Security Act created the executive Department of Homeland Security (DHS) and the position of Chief Information Officer.[1] The Chief Information Office was responsible for coordinating information sharing nationwide and for meeting other communications needs within DHS, throughout the federal government, and for

[1] P.L. 107-296, Sec. 103 (d) (2).

state and local first responders. Within DHS, several other initiatives were established to support emergency communications, especially as regards interoperability for first responders.

Title II created the Directorate for Information Analysis and Infrastructure Protection (IAIP), and established an Office of Science and Technology within the directorate. Duties of the Office of Science and Technology included research and development support for law enforcement agencies for "wire and wireless interoperable communications technologies."[2] Among the duties of the IAIP was the "preparation of a comprehensive national plan for securing the key resources and critical infrastructure" including . . . "emergency preparedness communications systems, and the physical and technological assets that support such systems."[3]

The National Communications System (NCS) was made responsible for telecommunications under the IAIP.[4] NCS was originally established at the Department of Defense by Executive Order in 1984 to assist the President, the National Security Council, the Director of the Office of Science and Technology Policy and the Director of the Office of Management and Budget in the exercise of the telecommunications functions and responsibilities, and the coordination of the planning for and provision of national security and emergency preparedness communications. NCS consults with the President's National Security Telecommunications Advisory Committee (NSTAC), among others, on issues related to national security and emergency preparedness for telecommunications. The primary focus of its programs is to assure communications links in times of crisis. Close cooperation with the telecommunications industry is also among NCS's responsibilities.

Responsibilities of the Directorate for Emergency Preparedness and Response (Title V) covered "comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology."[5]

DHS originally assigned primary responsibility for interoperable communications projects to the Wireless Public SAFEty Interoperable COMmunications Program—called Project SAFECOM, which was placed within the Science and Technology directorate.[6] Project SAFECOM had been authorized by the Office of Management and Budget (OMB) as one of 24 electronic government (e-government) initiatives. Responsibility for SAFECOM had been assigned by the OMB to the Wireless Directorate of the Department of the Treasury. At the recommendation of the Chief Information Officers of several federal agencies, including the Departments of Treasury, Commerce and Justice, Project SAFECOM was transferred to FEMA and followed it to DHS.[7]

The Secretary of Homeland Security assigned the responsibility of preparing a national strategy for communications interoperability to the Office of Interoperability and Compatibility (OIC), which DHS created, an organizational move that was later ratified by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004. SAFECOM operated as an entity within the OIC, which assumed the leadership role.

[2] P.L. 107-296, Sec. 232 (b) (6) (E).

[3] P.L. 107-296, Sec. 201 (d) (5).

[4] P.L. 107-296, Sec. 201 (g) (2).

[5] P.L. 107-296, Sec. 502 (7).

[6] "Homeland Security Starting Over with SAFECOM," Government Computer News, June 9, 2003.

[7] "FEMA Takes Lead for Broader Public Safety Wireless Program," Communications Daily, June 10, 2002.

In 2003, a CRS Report [8] discussed the evolving role of the Department of Homeland Security in providing support for public safety communications. At that time, concerns were expressed by public safety experts regarding the fragmented nature of the public safety information and communications network and the absence of a network overlay that could assure end-to-end communications across the country. Other concerns included the absence of redundancy in public safety networks and the lack of back-up locations for emergency communications.

Intelligence Reform and Terrorism Prevention Act of 2004

Acting on recommendations made in 2004 by the 9/11 Commission, Congress included several sections regarding improvements in communications capacity—including clarifications to the Homeland Security Act—in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458).

The Commission's analysis of communications difficulties on September 11, 2001, was summarized in the following recommendation.

> Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes. Furthermore, high-risk urban areas such as New York City and Washington, D.C., should establish signal corps units to ensure communications connectivity between and among civilian authorities, local first responders, and the National Guard. Federal funding of such units should be given high priority by Congress.[9]

Congress addressed both the context and the specifics of the recommendation for signal corps capabilities. The Intelligence Reform and Terrorism Prevention Act of 2004 amended the Homeland Security Act of 2002 to specify that DHS give priority to the rapid establishment of interoperable capacity in urban and other areas determined to be at high risk from terrorist attack. The law provided a statutory definition of interoperable communications as:

> the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another on demand, in real time, as necessary.[10]

The Secretary of Homeland Security was required to work with the Federal Communications Commission (FCC), the Secretary of Defense, and the appropriate state and local authorities to provide technical guidance, training, and other assistance as appropriate to achieve the goals established by the act. Minimum capabilities were to be established for "all levels of government agencies," first responders, and others, including the ability to communicate with each other.[11] The act further required the Secretary of Homeland Security to establish at least two trial programs in high-threat areas. The process of development for these programs was to contribute to the creation and implementation of a national model strategic plan.

---

[8] CRS Report RL31375, *Emergency Communications: Meeting Public Safety Spectrum Needs*, last updated July 1, 2003.

[9] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Washington: GPO, 2004, p. 397.

[10] P.L. 108-458, Title VII, Subtitle C, Sec. 7303, 118 STAT 3846.

[11] P.L. 108-458, Title VII, Subtitle C, Sec. 7303, 118 STAT. 3843 *et seq*.

Congress also raised the bar for performance and accountability, setting program goals for the Department of Homeland Security. Briefly, the goals were to:

- Establish a comprehensive, national approach for achieving interoperability;
- Coordinate with other federal agencies;
- Develop appropriate minimum capabilities for interoperability;
- Accelerate development of voluntary standards;
- Encourage open architecture and commercial products;
- Assist other agencies with research and development;
- Prioritize, within DHS, research, development, testing and related programs;
- Establish coordinated guidance for federal grant programs;
- Provide technical assistance; and
- Develop and disseminate best practices.

The act included a requirement that any request for funding from DHS for interoperable communications "for emergency response providers" be accompanied by an Interoperable Communications Plan, approved by the Secretary. Criteria for the plan were also provided in the act.[12]

The act also provided a sense of Congress that the next Congress—the 109th—should pass legislation supporting the Commission's recommendation to expedite the release of spectrum for public safety use. This was addressed in the Deficit Reduction Act of 2005 (P.L. 109-171).

The 9/11 Commission appeared to point the way toward a network solution along the lines of what was in place for military use. Its recommendation to use signal corps to assure connectivity in high-risk areas is apparently a reference to the Army Signal Corps. In testimony before Congress, Commissioner John F. Lehman commented on the lack of connectivity for first responders and referred to the "tremendous expertise" of the Department of Defense (DOD) and its capabilities in procurement, technology and research and development. Referring specifically to the Army Signal Corps, Mr. Lehman suggested that the DOD should have responsibility to provide "that kind of support to the first responders in the high-target, high risk cities like New York."[13] Building on the concept of using the Army Signal Corps as a model, the law directed the Secretary to consult with the Secretary of Defense in the development of the test projects, including review of standards, equipment, and protocols.[14]

The Homeland Security Appropriations Act, 2007

The destruction caused by Hurricanes Katrina and Rita in August-September 2005 reinforced recognition of the need for providing interoperable, interchangeable communications systems for public safety and also revealed the potential weaknesses in existing systems to withstand or recover from catastrophic

[12] P.L. 108-458, Title VII, Subtitle C, Sec. 7303 118 STAT. 3843 *et seq*.

[13] Testimony of Commissioner John F. Lehrnan, National Commission on Terrorist Attacks Upon the United States, Hearing, House of Representatives, Committee on Government Reform, "Moving from 'Need to Know' to 'Need to Share', "August 3,2004.

[14] P.L. 108-458, Title VII, Subtitle C, Sec. 7304, 118 STAT. 3847-3848.

events. Testimony at numerous hearings following the hurricanes suggested that DHS was responding minimally to congressional mandates for action, most notably as expressed in the language of the Intelligence Reform and Terrorism Prevention Act of 2004. Bills subsequently introduced in both the House and the Senate proposed strengthening emergency communications leadership and expanding the scope of the efforts for improvement. Some of these proposals were included in Title VI of the Homeland Security Appropriations Act, 2007 (P.L. 109-295). Title VI—the Post-Katrina Emergency Management Reform Act of 2006— which reorganized the Federal Emergency Management Agency (FEMA), gave the agency new powers, and clarified its functions and authorities within DHS.[15]

The 21st Century Emergency Communications Act of 2006 and the Office of Emergency Communications

The Homeland Security Appropriations Act, 2007 also addressed public safety communications in Title VI, Subtitle D—the 21st Century Emergency Communications Act of 2006. This section created an Office of Emergency Communications (OEC) and the position of Director, reporting to the Assistant Secretary for Cybersecurity and Communications. As described in the legislation, the purpose of the OEC was to marshal the efforts of DHS agencies and to work with other agencies and departments in developing effective solutions for emergency communications. The Director was required to take numerous steps to coordinate emergency communications planning, preparedness, and response, particularly at the state and regional level. The Director was also required to work with the National Communications System in the establishment of a "national response capability with initial and ongoing planning, implementation, and training for the deployment of communications equipment for relevant State, local, and tribal governments and emergency response providers in the event of a catastrophic loss of local and regional emergency communications services."[16]

Other responsibilities assigned to the Director included conducting outreach programs, providing technical assistance, coordinating regional working groups, promoting the development of standard operating procedures and best practices, establishing nonproprietary standards for interoperability, developing a National Emergency Communications Plan, working to assure operability and interoperability of communications systems for emergency response, and reviewing grants.

The National Emergency Communications Plan (NECP) was to "(1) 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"(2) ensure, accelerate, and attain interoperable emergency communications nationwide."[17]

Required elements of the plan included establishing requirements for assessments and reports, and an evaluation of the feasibility of developing a mobile communications capability modeled on the Army Signal Corps. The feasibility study was to be done by DHS on its own or in cooperation with the Department of Defense. Congress also required assessments of emergency communications capabilities, including an inventory that identified radio frequencies used by federal departments and agencies.[18]

---

[15] Information on the FEMA reorganization is provided in CRS Report RL33729, *Federal Emergency Management Policy Changes After Hurricane Katrina: A Summary of Statutory Provisions*, coordinated by Keith Bea.

[16] P.L. 109-295, Title VI, Sec. 671(b), 'Title XVIII, 'Sec. 1801, (c) (9), 120 STAT. 1434

[17] P.L. 109-295, Title VI, Sec. 671(b), 'Title XVIII, 'Sec. 1802, (a) (1) and (2), 120 STAT. 1436.

[18] P.L. 109-295, Title VI, Sec. 671(b), 'Title XVIII, 'Sec. 1803, 120 STAT. 1437-1438.

Planning efforts were to include coordination with Regional Administrators appointed by the FEMA Administrator to head ten Regional Offices. To assist these efforts, Congress required the creation of Regional Emergency Communications Coordination (RECC) Working Groups.[19] These groups were to provide a platform for coordinating emergency communications plans among states and were intended to include representatives from many sectors with responsibility for public safety and security. The formation of the regional working groups, the RECCs, responded in part to requests from the public safety community to expand interoperable communications planning to include the second tier of emergency workers. Nonfederal members of the RECC were to include first responders, state and local officials and emergency managers, and public safety answering points (911 call centers). Additionally, RECC working groups were to coordinate with a variety of communications providers (such as wireless carriers and cable operators), hospitals, utilities, emergency evacuation transit services, ambulance services, amateur radio operators, and others as appropriate.

DHS and Other Federal Agencies

Federal legislative requirements for actions by the Department of Homeland Security in support of public safety communications has, from the first law that created the Department, assigned similar responsibilities to multiple agencies within DHS. Furthermore, legislation has required that DHS initiatives for public safety be coordinated with other agencies. Many would argue that shortcomings in the coordination of programs across agencies and departments have undermined leadership and diluted the effectiveness of some programs.

Congress has separately and specifically given authority to DHS and to the FCC to act on behalf of public safety. In the case of DHS, authority includes planning and implementing public safety communications solutions and setting requirements to coordinate and support specific goals, such as interoperability and a national communications capability.

By 2006, three federal agencies were proposing different approaches to provide communications interoperability for public safety.[20] The FCC was moving forward with a proposal for a public-private partnership to build a nationwide network,[21] and later included a similar plan for building the network in its *National Broadband Plan*.[22] The National Telecommunications and Information Administration (NTIA) established a Spectrum Advisory Committee whose objectives included developing spectrum-efficient recommendations for a national network of networks.[23] Within DHS, the focus was on gateways—also known as bridges, or as cross-talk or cross-patch systems, among other terms. The gateway is a "black box" that can accept wireless transmissions on one frequency standard and resend them on other frequency standards. As a result, they are inefficient users of spectrum, since a single message is using two or more frequency assignments. Gateways are the technology centerpiece of efforts

[19] P.L. 109-295, Title VI, Sec. 671(b), 'Title XVIII, 'Sec. 1805, 120 STAT. 1439.

[20] Described in CRS Report RL33838, *Emergency Communications: Policy Options at a Crossroads*, by Linda K. Moore, last updated January 30, 2007.

[21] Congressionally mandated obligations of the FCC include to "promote safety of life and property through the use of wire and radio communication," (47 U.S.C.§ 151) and requirements regarding the assignment of radio frequencies for public safety use. The FCC created a Public Safety and Homeland Security Bureau in 2006 to consolidate its many programs oriented toward public safety.

[22] FCC, *Connecting America: The National Broadband Plan, 2010.*

[23] The NTIA manages radio frequency spectrum allocated for federal use and advises the Administration on spectrum issues and new wireless technologies, among other responsibilities.

by DHS to achieve situational interoperability.[24] Situational interoperability and "response-level emergency communications" remains an important goal for DHS and the OEC, according to recently reported findings and recommendations.[25] For the purposes of the NECP, response-level communications is "the capacity of individuals with primary operational leadership responsibility to manage resources and make timely decisions during an incident." The Office of Emergency Communications has advocated emergency communications planning from the bottom up, encouraging stakeholders to find their own solutions within frameworks established within DHS, evolving along a development continuum provided by the agency.[26] A primary activity of the OEC is to manage statewide planning and coordination for interoperable communications and administer compliance with the *National Emergency Communications Plan.*

According to testimony in 2008, neither the FCC nor the OEC undertook to incorporate each other's goals in their specific planning processes.[27] In 2009, the Government Accountability Office confirmed the lack of coordination and cooperation between DHS and the FCC.[28] In April, 2010, the FCC established the Emergency Response Interoperability Center (ERIC).[29] ERIC has been tasked with implementing standards for national interoperability and developing technical and operational procedures for the public safety wireless broadband network. DHS is to participate in public safety outreach and technical assistance, as well as best practices development, through its Office of Emergency Communications. It is intended for ERIC to work closely with the Public Safety Communications Research program, jointly managed by the National Institute of Standards and Technology (NIST) and the NTIA, to develop and test the technological solutions needed for public safety broadband communications.[30] ERIC has, in part, become the forum for cooperation among three agencies with different visions of the future and competing claims to provide leadership.

President's National Security Telecommunications Advisory Committee

In January 2010, the President's National Security Telecommunications Advisory Committee (NSTAC) received an Executive Order requiring a report on communications resiliency, that would include recommendations for immediate action and a study of what types of networks would be in place five to ten years in the future.[31] One of the recommendations was to encourage DHS to file comments with the FCC in support of continuing efforts to work closely with industry "as it builds the nationwide

[24] See, for example Department of Homeland Security Press Conference on Assessment of Interoperable Communications, January 3, 2007 (transcript provided by Federal News Service), and Homeland Security Press release, "Remarks by Homeland Security Secretary Michael Chertoff at the Tactical Interoperable Communications Conference," May 8, 2006.

[25] Department of Homeland Security, *National Emergency Communications Plan: Urban Area Communications Key Findings and Recommendations*, 2011.

[26] The continuum diagram is at http://www.safecomprogram.gov/SAFECOM/Tools/Continuum/continuum.htm; additional descriptions at http://www.safecomprogram.gov/SAFECOM/oecguidancedocuments/continuum/default.htm.

[27] Oral and written testimony before the House Committee on Homeland Security, Subcommittee on Emergency Communications, Preparedness, and Response, "Interoperability in the Next Administration: Assessing the Derailed 700 MHz D Block Public Safety Auction," September 16, 2008.

[28] GAO, *Emergency Communications: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts*, GAO-09-604, June 26, 2009.

[29] FCC, *Order*, PS Docket No. 06-229, released April 23, 2010 at http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-10-67A1.pdf.

[30] NIST, "Demonstration Network Planned for Public Safety 700 MHz Broadband," December 15, 2009.

[31] *NSTAC Report to the President on Communications Resiliency*, April 19, 2011.

interoperable public safety mobile broadband network. . . ."[32] The *Report*'s scenario for the "Public Safety Communications in Network 2015" assessed the current status of public safety communications as follows:

> While many state and local agencies have modernized and expanded their mission-critical voice systems through initiatives such as federal grant programs, or are in the process of doing so, the communications challenges for those operating on the front lines in public safety have not been eliminated.[33]

The key public safety communications trends in 2015 identified by the report are: public safety system consolidation; interoperability, convergence and roaming; future broadband wireless network; emerging capabilities; specialized public and private devices; and emergency alerting capabilities. These trends might be addressed in a future version of the National Emergency Communications Plan and could have been included in the plan published in 2008, as all of the identified trends were already well-established by public dialogs about communications technology.

Funding Interoperable Communications

It was not until after September 11, 2001 that federal agencies began to give a high priority to programs that improved emergency communications and interoperability, to direct grants specifically for interoperable communications, and to provide totals for grants directed to these types of programs. A number of federal agencies have roles in guiding and monitoring some decisions of states and localities through grant administration, greatly diffusing federal oversight and leadership through grant governance. There are currently over 40 active programs, administered by nine different departments and multiple agencies within those departments, providing grants for funding emergency communications.[34] Within DHS, the Office of Emergency Communications, the SAFECOM Program, and the Federal Emergency Management Administration (FEMA) are among the agencies that formulate policies, plan exercises, provide guidelines, and establish requirements.[35]

Because of the proliferation of grant programs and earmarks, and because of varying levels of details in published information regarding federal grant programs, it seems difficult to prepare an accurate accounting of what has been spent and how, and the Congressional Research Service was unable to locate such an accounting.[36] Based on CRS research, there does not appear to be available information to assess planning within the Department of Homeland Security for funding specific infrastructure goals, such as radio tower construction, that would contribute to the development of interoperable network connectivity nationwide. This approach would appear to fit with the DHS policy that planning for emergency communications should be from the bottom up, evolving along a development continuum provided by the

[32] *Report*, page ES-2.

[33] *Report*, page 12.

[34] Based on a summary of federal programs provided by SAFECOM.

[35] Links to relevant SAFECOM and FEMA grant program documents are available at http://www.safecomprogram.gov/SAFECOM/grant/default.htm. Information on OEC grants is at http://www.dhs.gov/xopnbiz/grants/gc_1288707294166.shtm.

[36] CRS, Congressional Distribution Memorandum, "Federal Funding of State and Local Emergency Communications Projects," updated June 10, 2011.

agency.[37] Planning for interoperability at the federal level should be primarily through goal-setting, such as those established in the *National Emergency Communications Plan,*[38] not through direct leadership.

Conclusion

After September 11, 2001, there was a shared sense in Congress and throughout the nation that the communications capabilities available to first responders were inadequate and needed to be improved. The problems were understood, but not the answers. In 2004, Congress had identified specific actions to be taken by the Department of Homeland Security in support of communications interoperability, which was defined in the Intelligence Reform and Terrorism Prevention Act of 2004 as operating " . . . through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another on demand, in real time, as necessary." Many policy advisers within the public safety community were recommending some form of network to provide an interoperable communications solution. By 2005, the commercial wireless industry and the Department of Defense were planning on how to utilize new network technologies based on the Internet Protocol. In 2006, the FCC proposed a public-private partnership to build a network for public safety that would use new broadband technologies to provide voice, data, and video communications. A consensus in favor of a network solution had therefore begun to emerge. In recognition of the potential role of new network technologies to provide interoperable, resilient, and effective support for public safety communications, the 21st Century Emergency Communications Act of 2006 created the Office of Emergency Communications. The law required the OEC to develop a national plan that was to "ensure, accelerate, and attain interoperable emergency communications nationwide," and provided DHS with new tools to complete the plan. Still, consensus was not universal, and many stakeholders within the public safety community in particular remained uncommitted to the concept of using a nationwide network to meet their primarily local needs. The debates about a network solution revealed uncertainty among policy makers and stakeholders regarding the appropriate role of the federal government. This debate appears to remain unresolved: bills that have been introduced in the 112th Congress show a great deal of cohesion about the need for a nationwide network and what type of support it should provide to public safety agencies, but little agreement about the roles that different federal agencies would play in the deployment and operation of the network.

[37] The continuum diagram is at http://www.safecomprogram.gov/SAFECOM/Tools/Continuum/continuum.htm; additional descriptions at http://www.safecomprogram.gov/SAFECOM/oecguidancedocuments/continuum/default.htm.

[38] DHS, *National Emergency Communications Plan*, July 2008.