Public Safety Communications: Policy, Proposals, Legislation and Progress

Updated February 23, 2005

Linda K. Moore
Analyst in Telecommunications Policy
Resources, Science, and Industry Division
Summary

Since September 11, 2001, the effectiveness of America’s communications capabilities in support of the information needs of first responders and other public safety workers has been a matter of concern to Congress. The National Intelligence Reform Act of 2004 (P.L. 108-458) included sections that responded to recommendations made by the 9/11 Commission, in its report of July 2004, and by others in recent years, regarding public safety communications. The act requires several pilots and studies that will provide new information to Congress about public safety communications needs and access to spectrum for wireless technologies, two issues addressed by the Commission. The act also tightens governance of some federal programs relating to public safety communications.

This report provides an analysis of major policy questions regarding public safety communications. The 9/11 Commission recommendations for action to improve communications and the testimony and comments of experts provide a framework to review what has been accomplished since September 11, what legislative initiatives Congress may plan for the 109th Congress, and longer term goals and concerns. The major conclusions that may assist policy makers are that (1) there is a need to unify spectrum policy and communications policy at every level; (2) the 9/11 Commission recommendation to use signal corps skills and technology sums up a decade of recommendations from public safety experts; and (3) federal actions taken to-date are judged by most to be inadequate. Criticisms from the public safety community include the failure to release spectrum for public safety communications; the failure to provide a policy that encourages the implementation of newer wireless technologies (some of which may require new spectrum allocations); the slow pace of development for technical and operational standards for interoperability; and the unmet needs for communications support in high-risk, urban areas. All of these criticisms have been addressed in some form by provisions in the act, which establishes goals and deadlines for these measures for 2005 and later years. In particular, both Congress and the Administration have set requirements for the Department of Homeland Security that include a strategy for spectrum use and its role in public safety communications.
Contents

National Intelligence Reform Act .......................................................... 1
  Spectrum Allocation ............................................................................... 2
    Sense of Congress .............................................................................. 2
  Improving Spectrum Capacity for Public Safety ................................. 3
    The Cost of Fragmentation ................................................................ 4
  Communications Support and Interoperability ...................................... 5
    Funding ............................................................................................ 6
  High-Risk Urban Areas ....................................................................... 7

Policy and Planning ........................................................................... 8
  Federal Planning .................................................................................. 9
  State Planning ................................................................................... 9

Policy and Technology ........................................................................ 10

Policy and Progress ........................................................................... 12
  Convergence ...................................................................................... 13

Appendix I - Federal Administration ................................................... 16
  National Telecommunications and Information Administration .......... 16
  Federal Communications Commission ............................................... 17
    Homeland Security ........................................................................... 17
    Spectrum and Interoperability ......................................................... 17
  Department of Homeland Security, Office of Interoperability and
    Compatibility ..................................................................................... 18
    SAFECOM ........................................................................................ 18
  Regional Technology Integration Initiative ......................................... 19
  National Incident Management System .............................................. 20
  Other Coordinating Bodies .................................................................. 20
Public Safety Communications: Policy, Proposals, Legislation and Progress

Public safety agencies include the nation’s first responders (such as firefighters, police officers, and ambulance services) and a number of local, state, federal — and sometimes regional — authorities. Communications, often wireless radios, are vital to these agencies’ effectiveness and to the safety of their members and the public. Wireless technology requires radio frequency capacity in order to function, and existing wireless technology is designed to work within specified frequency ranges.

Different operations, different applications, different rules and standards, and different radio frequencies are among the problems first responders face in trying to communicate with each other. Interoperability, also referred to as compatibility or connectivity, refers to the capability for different systems to readily contact each other. Facilitating interoperability has been a policy concern of public safety officials for a number of years.1 Since September 11, 2001 — when communications failures added to the horror of the day — achieving interoperability for public safety communications has become an important policy concern for Congress.

National Intelligence Reform Act

The National Commission on Terrorist Attacks Upon the United States (9/11 Commission) 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.2

The Commission, in this paragraph, recognized the important link between access to spectrum and the effectiveness of communications technology. Briefly, the recommendations says:

- free up and assign more spectrum for public safety use;

---

1 Difficulties in communications after a major plane crash in the Potomac River in January 1982 is often cited as the impetus for expanding interoperability in the Capital Area.

• establish communications support (the role of a signal corps typically is to provide information systems and networks for real-time command and control);
• with interoperable communications (connectivity); and
• fund these communications operations for high-risk urban areas.

The 9/11 Commission recommendations for public safety are a pithy summation of issues raised in the last decade or so. Provisions in the act that respond to the recommendations of the Commission and of the public safety community, among others, are discussed below.

**Spectrum Allocation**

The Balanced Budget Act of 1997 requires the Federal Communications Commission (FCC) to allocate 24 MHz of spectrum at 700 MHz to public safety, without providing a hard deadline for the transfer. The channels designated for public safety are among those currently held by TV broadcasters; they are to be cleared as part of the move from analog to digital television (DTV). The 9/11 Commission report regarding spectrum availability speaks directly to the issue of the 700 MHz spectrum that has been assigned to public safety but is not yet available. It recommended that Congress pass legislation that would free those channels. Although the task of freeing spectrum for public safety could be addressed as a separate issue, actions so far have focused primarily on the steps to be taken for releasing all the encumbered spectrum while assuring access to broadcast television programs.

**Sense of Congress.** The National Intelligence Reform Act provides the sense of Congress that it “must act to pass legislation in the first session of the 109th Congress that establishes a comprehensive approach to the timely return of analog broadcast spectrum as early as December 31, 2006,” and that any delay “will delay the ability of public safety entities to begin planning to use this needed spectrum.” Although the Senate version of the intelligence bill (S. 2845, 108th) included a provision that would have released in a timely manner those channels needed for public safety communications, the House of Representative’s preference to address the issue in its entirety prevailed. Some of the possible actions that Congress may decide to take could include using spectrum auction proceeds to subsidize the purchase of set-top signal converter boxes, thereby allowing analog broadcasts to

---

3 Radio frequency spectrum is measured in hertz. Radio frequency is the portion of electromagnetic spectrum that carries radio waves. The distance an energy wave takes to complete one cycle is its wavelength. Frequency is the number of wavelengths measured at a given point per unit of time, in cycles per second, or hertz (Hz). Typical designations are: kHz — kilohertz or thousands of hertz; MHz — megahertz, or millions of hertz; and GHz — gigahertz, or billions of hertz. Bandwidth refers generally to the capacity of channels to carry voice and data, a function of technology and the amount of spectrum assigned. Most frequency assignments for first responders are narrowband and most channels currently in use are located below 512 MHz.

4 P.L. 108-458, Title VII, Subtitle E, Sec. 7501 (b) (1).

5 P.L. 108-458, Title VII, Subtitle E, Sec. 7501 (b) (2).
continue indefinitely without cutting viewer access;\textsuperscript{6} endorsing plans by the FCC to change the criteria for freeing 700 MHz channels; or a rewriting of the provisions of the Balanced Budget Act that govern transition plans.\textsuperscript{7}

**Improving Spectrum Capacity for Public Safety**

The act requires the FCC, in consultation with the Secretary of Homeland Security and the National Telecommunications and Information Administration (NTIA),\textsuperscript{8} to conduct a study on the spectrum needs for public safety, including the possibility of increasing the amount of spectrum at 700 MHz.\textsuperscript{9} This provision is responsive to the many public safety officials who believe that additional spectrum should be assigned for public safety use — and not exclusively for first responders.\textsuperscript{10} In addition to providing spectrum for other types of users, the spectrum available for public safety should be able to support high-speed transmissions capable of quickly sending data (such as photographs, floor plans and live video). This requires providing frequencies with greater bandwidth to enable wireless broadband and new-generation technologies. Although radio frequencies have been designated for state and local public safety use in the 700 MHz range, there are no allocations specifically for federal use at 700 MHz and the bandwidth assignments are judged by most experts to be too narrow for full broadband. Many have advocated that additional spectrum be allocated at 700 MHz to accommodate federal users and to support newer, broadband wireless technologies as part of a nationwide network for public safety communications. The Spectrum Coalition for Public Safety has circulated proposed legislation that would allocate additional spectrum at 700 MHz for use by state and local first responders, critical infrastructure industries, and federal public safety agencies.\textsuperscript{11}

\textsuperscript{6} The Administration reportedly has opposed this approach, see, for example, “White House Opposes DTV Subsidy Proposal,” by Donny Jackson, TelephonyOnline.com, October 22, 2004.

\textsuperscript{7} Details are provided in CRS Report RL32622, *Public Safety, Interoperability and the Transition to Digital Television*.

\textsuperscript{8} The NTIA, Department of Commerce, administers federal use of spectrum.

\textsuperscript{9} P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (a).

\textsuperscript{10} In 1997 amendments to the Communications Act of 1934, Congress defined public safety services as “services — (A) the sole or principal purpose of which is to protect the safety of life, health or property; (B) that are provided (i) by State or local government entities; or (ii) by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and (C) that are not made commercially available to the public by the provider.” [47 U.S.C. § 337 (f)(1)]. The National Intelligence Reform Act uses the more restrictive definition of first responders as provided in the Homeland Security Act of 2002 (6 U.S.C. 101).

\textsuperscript{11} Spectrum Coalition for Public Safety at [http://www.spectrumcoalition.org].
Although, cumulatively, radio frequencies designated for non-federal public safety total over 90 MHz,\(^{12}\) the characteristics of these frequencies are dis-similar, requiring different technological solutions. The fragmentation of spectrum assignments for public safety is a significant barrier to achieving interoperability in the future and, in the past, has been one of many of the technical problems that plague public safety communications, such as out-of-date equipment, proprietary solutions, congestion and interference. The immediate barrier to achieving radio communications interoperability is — simply put — that UHF and VHF frequencies\(^{13}\) cannot connect directly with each other; and older, analog equipment widely used below 512 MHz cannot connect with newer digital equipment at 800 MHz. Technology for new frequencies at 4.9 GHz is still in the early stage of development but these frequencies appear suitable primarily for short-range transmission. None of the above frequency assignments can, using current technology, support wide-area communications relying on high-speed, data-rich transmissions.

The need for greater spectral capacity will grow with the number of participants in interoperable systems and the amounts of information being shared on these systems. Bottlenecks in communications are a problem that is already manifest among federal computer networks and landline transmissions, and many believe it will worsen as more information is pushed through. As emergency response units become more mobile, demand for time-critical, wireless communications capacity will also increase. New technologies that improve communications capacity are being introduced almost continuously, but the need to provide suitable spectrum for a full range of voice and data communications will persist.

**The Cost of Fragmentation.** The number of radio frequencies available for interoperable communications capability can significantly impact first responder communications, and the range of these frequencies can significantly impact the cost of equipment. Manufacturers cite short production runs for wireless handsets as one of the causes for higher costs associated with public safety communications equipment. (An analog walkie-talkie might cost $300, a “typical” price). A radio with limited interoperability that meets Project 25 standards\(^{14}\) might cost as much as $3,000 in a limited production run. Purchasing “cross-talk” equipment that provides interoperability by linking radio frequencies through a black box can run into the millions of dollars. Therefore, many argue that creating common, interoperable

---

\(^{12}\) Estimated at approximately 97 MHz in Testimony of Michael K. Powell, Chairman, Federal Communications Commission, at Hearing of Senate Committee on Commerce, Science and Transportation, “Spectrum for Public Safety Users,” September 8, 2004. The NTIA has apparently not supplied a similar estimate of frequencies assigned to federal agencies that are or can be accessed for public safety purposes.

\(^{13}\) Very High Frequency (VHF) and Ultra High Frequency (UHF) are transmitted in three bands in the United States — low VHF, high VHF and UHF.

channels at 700 MHz is cost-effective as well as organizationally and technologically desirable.15

Communications Support and Interoperability

The 9/11 Commission 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.”16

The role of a signal corps typically is to provide information systems and networks for real-time command and control. The Army maintains mobile units to provide capacity and specialized support to military operations, worldwide. According to the U.S. Army Info Site on the Internet

The mission of the Signal Corps is to provide and manage communications and information systems support for the command and control of combined arms forces. Signal support includes Network Operations (information assurance, information dissemination management, and network management) and management of the electromagnetic spectrum. Signal support encompasses all aspects of designing, installing, maintaining, and managing information networks to include communications links, computers, and other components of local and wide area networks. Signal forces plan, install, operate, and maintain voice and data communications networks that employ single and multi-channel satellite, tropospheric scatter, terrestrial microwave, switching, messaging, video-teleconferencing, visual information, and other related systems. They integrate tactical, strategic and sustaining base communications, information processing and management systems into a seamless global information network that supports knowledge dominance for Army, joint and coalition operations.17

The Army Signal Corps is intended to provide a communications backbone, a core network, with important elements such as spectrum management, the operation of communications centers, and support of communications networks that include both large area regional communications and radio coverage for local wireless interoperability. The Corps’ communication backbone delivers connectivity on site

15 Speakers at a CRS-sponsored seminar provided equipment cost estimates and were among those who have confirmed the need for access to spectrum at 700 MHz as part of the solution for achieving interoperability. Public Safety Communications: Interoperability Technology Workshop, November 17, 2003.


among combined forces and connectivity to command centers. These operations are scalable and can be deployed when and where needed.

A discussion of key federal programs to support communications and foster interoperability is included in the Appendix of this report. At the end of the 108th Congress, the goals and accomplishments of these programs were less ambitious than the signal corps template provided by the 9/11 Commission. Congress responded to the Commission’s recommendations with language in the National Intelligence Reform Act that raises the bar for performance and accountability, as well as easing some of the obstacles to performance. Among the program goals the act sets for the Department of Homeland Security and the Federal Communications Commission are

- develop comprehensive, national approach for achieving interoperability.
- coordinate with other federal agencies.
- establish 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 for research, development, testing and related programs.
- establish coordinated guidance for federal grant programs.
- provide technical assistance.
- develop and disseminate best practices.
- establish performance measurements and milestones for systematic measurement of progress.\(^ {18}\)

The act also instructs the Secretary of Homeland Security to lead a study to “assess strategies that may be used to meet public safety telecommunications needs.”\(^ {19}\) The strategies study is to address the need for nationwide interoperable communications networks, the capacity of public safety to use wireless broadband applications, and the communications capabilities of “all emergency response providers. . . .” The use of “commercial wireless technologies to the greatest extent possible” is to be considered.

**Funding.** Grants that have helped to pay for new programs for interoperability have come from a number of federal sources, notably from Department of Justice programs and, within the Department of Homeland Security (DHS), from the Federal Emergency Management Administration (Emergency Preparedness and Response Directorate) and the Office for Domestic Preparedness (ODP) in the Border and Transportation Security Directorate. Grant programs such as those at ODP for Urban Area Security and High-Threat Urban Areas are on-going.\(^ {20}\)

---

\(^ {18}\) P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (a) (1).

\(^ {19}\) P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (b).

\(^ {20}\) For full details, please refer to CRS Report RS21677, Office for Domestic Preparedness Grants for 2004: State Allocation Fact Sheet and CRS Report RL32696, Fiscal Year 2005 (continued...).
According to an undated fact sheet from DHS, since September 11, 2001, the Administration has allocated $200 million specifically for improving interoperability and $5.4 billion has been provided to states for emergency preparedness that could include interoperable communications. The amount of dollars available, although significant, represents a small portion of the “several billions” that the GAO reports as the estimated sum needed to achieve interoperability. Although the need for funding appears to be at the top of almost any list regarding interoperability policy, many have expressed concern that there is no strategy that prioritizes what needs to be funded though federal programs, leading to waste and inequities. The GAO reports that “federal funding assistance programs to state and local governments do not fully support regional planning for communications interoperability.” The restraints imposed by limiting funding to annual grants was cited as one cause. Provisions of the National Intelligence Reform Act permit multi-year commitments to fund interoperable communications for up to three years, with a ceiling of $150 million for future obligations.

The act authorizes annual sums in the low $20 millions for each fiscal year from 2005 through 2009. The 2005 authorization is $22,105,000; the amount rises each year to $24,879,000 in 2009. These sums are to be used for efforts to improve interoperability and to assist interoperable capability in high-risk urban areas.

**High-Risk Urban Areas**

The 9/11 Commission recommendation urged immediate funding of signal corps in high-risk urban areas to assure connectivity “among civilian authorities, local first responders, and the National Guard.” The act responded by amending the Homeland Security Act to specify that DHS is to give priority to the rapid establishment of interoperable capacity in urban and other areas determined to be at high risk from terrorist attack. The Secretary of Homeland Security is required to work with the FCC, the Secretary of Defense, and appropriate state and local authorities to provide technical guidance, training, and other assistance as appropriate. Minimum capabilities for “all levels of government agencies,” first responders, and others include the ability to communicate with each other and to

---

20 (...continued)


23 Ibid., Highlights.

24 P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (e).

25 P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (d), ‘Sec. 510 ‘(a).
have “appropriate and timely access” to the Information Sharing Environment, an initiative treated elsewhere in the act.\(^{26}\)

The act further requires the Secretary of Homeland Security to establish at least two pilot programs in high threat areas. The process of development for these programs is to contribute to the creation and implementation of a national model strategic plan.\(^{27}\) The purpose of this plan is to foster interagency communications at all levels of the response effort.\(^{28}\) Building on the 9/11 Commission recommendation to use the resources of the Army Signal Corps, the Secretary is to consult with the Secretary of Defense in the development of the pilot projects, including review of standards, equipment and protocols.\(^{29}\)

**Policy and Planning**

At a number of hearings throughout the 108th Congress,\(^{30}\) and in reports by the General Accounting Office,\(^{31}\) the need for better governance and planning for interoperability was raised repeatedly. While not embracing the 9/11 Commission recommendation for a Signal Corps, the National Intelligence Reform Act does include requirements for planning and for studies and reports that might lead to future changes in governance and national policy for interoperability and planning. The Administration also has asked for detailed studies and plans regarding spectrum use and communications for public safety.

\(^{26}\) P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (d), ‘Sec. 510 ‘(b).

\(^{27}\) P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (a).

\(^{28}\) P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (b).

\(^{29}\) P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (d).


Federal Planning

On November 30, 2004, President George W. Bush issued a memorandum to the heads of Executive Departments and agencies regarding steps to be taken to improve the management of spectrum assigned for federal use.32 Most of these steps are to implement recommendations made by the Federal Government Spectrum Task Force in its report to the President in June 2004.33 Among the deadlines provided in the memorandum are two requirements related specifically to public safety. One requirement is for the Secretary of Homeland Security to identify public safety spectrum needs by June 2005. The Secretary is to work with the Secretary of Commerce and, as needed, with the Chairman of the Federal Communications Commission; representatives from the public safety community; state, local, regional and tribal governments; and the private sector. Also, by year-end 2005, the Secretary of Homeland Security is to lead the preparation of a Spectrum Needs Plan, “to address issues related to communication spectrum used by the public safety community, as well as the continuity of Government operations.” Concurrently, the Secretary of Commerce is to develop a Federal Strategic Spectrum Plan.

State Planning

The National Intelligence Reform Act links grant-making with planning efforts in its provisions.34 Requirements for planning for spectrum and interoperability in order to qualify for funding assistance include 1) description of available radio frequency uses and planned uses;35 2) description of how plans for spectrum use and interoperability are compatible with plans for “Federal, State and local governmental entities, military installations, foreign governments, critical infrastructure, and other relevant entities;”36 and 3) inclusion of a five-year plan showing how resources will be used.37 The language provides criteria for non-federal planners that could be expected to mesh with federal planning efforts required by the Administration and in other sections of the act.38 Furthermore, additional provisions of the act require the Secretary of Homeland Security to establish at least two pilots to develop a “regional strategic plan to foster interagency communications,” consistent with the

34 Funding programs are covered in several CRS reports, including CRS Report RL32696, Fiscal Year 2005 Homeland Security Grant Program: State Allocations and Issues for Congressional Oversight, by Shawn Reese.
35 P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (f) (2).
36 P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (f) (3).
37 P.L. 108-458, Title VII, Subtitle C, Sec. 7303 (f) (4).
38 Notably, P.L. 108-458, Title VII, Subtitle E, Sec. 7502.
national strategic plan to be developed at the request of Congress by the Secretary of Homeland Security.\textsuperscript{39}

The strategic planning efforts required by Congress and by the Administration have similar goals. Although requirements for federal planning are more extensive than what has been asked of states and other non-federal entities, a possible synergy among the various programs could lead to the crafting of a nationwide plan with clearly defined links to state and local planning and to the private sector. A template for interoperability planning has been developed within DHS that could be used as a first step toward meeting the planning requirements set forth in the act.\textsuperscript{40}

\textbf{Policy and Technology}

The act requires the Secretary of Homeland Security, the FCC, and the NTIA to conduct a study to assess strategies for public safety communications. The study is to include

- the need and efficacy of deploying nationwide interoperable communications networks
- the capacity of public safety entities to use wireless broadband applications
- the communications capabilities of all emergency response providers, including hospitals and health care workers, and current efforts to promote communications coordination and training among emergency response providers.\textsuperscript{41}

Conclusions from this assessment might lead to recommendations for the development of a nationwide network for public safety communications, as many have advocated.\textsuperscript{42} The 9/11 Commission proposed a signal corps approach to public safety communications and urged that this be provided to high-risk urban areas. Such a capability would seem to include a system architecture to provide a backbone for wide area and local area networks and to support interoperability system-wide, as needed.

In addition to local gateways, communities — and the military — are testing leading edge technologies that can overcome problems of limited capacity of assigned frequencies, incompatible standards and other technical problems. The

\textsuperscript{39} P.L. 108-458, Title VII, Subtitle C, Sec. 7304 (b).
\textsuperscript{41} P.L. 108-458, Title VII, Subtitle E, Sec. 7502 (b).
\textsuperscript{42} For example, testimony of Gary Grube, Chief Technology Officer, Motorola, Inc. at Hearing of Senate Committee on Commerce, Science and Transportation, “Spectrum for Public Safety Users,” September 8, 2004.
technologies being tested to improve interoperability include software-driven radios and smart antennae, mesh networks, and cognitive radio.

Software defined networks (radios, base stations, antennae) move wireless communications away from hard-wired equipment, where functionality is built into the components at the factory, by allowing changes in parameters to be downloaded remotely. Parameters that can be changed include standards and frequency assignments. Cognitive radio has the potential to eliminate entirely the need for frequency assignments. Cognitive radio is able to seek out and use any available frequency through miniaturized software programs contained within radio equipment. Advanced versions of software-defined radio (SDR) being tested today are the building blocks for commercial applications of cognitive radio.

The Department of Defense, its agencies, and military departments have been leaders in research and development for software-programmable radios and base centers. These new technologies are expected to provide seamless interoperability in tactical operations and decrease the cost of infrastructure. A key program is the Joint Tactical Radio System (JTRS), designed to help the military migrate from its current wireless technology to SDR. DOD is promoting the use of JTRS and its software communications architecture for homeland security and public safety communications and interoperability.

Mesh networking is another promising technology that can facilitate public safety communications and interoperability. Mesh networks use radios that also act as mobile antennae, eliminating dependency on fixed antenna. Cities that are trying mesh networks for public safety include Medford, Oregon; San Mateo, California; North Miami Beach, Florida; and Garland, Texas. Other communities are using unlicensed spectrum to use Wi-Fi networks (fixed antennae) for public safety communications. Using commercial, third-generation (3G) wireless technologies is also an option for first responders. New 3G phones offer high-speed Internet access and image transmissions as well as voice communications. Off-the-shelf camera phones can relay photos from an incident site to a command center, or vice versa. Advanced mobile phones are being prepared to receive multi-channel TV broadcasts in test markets. Interoperability for commercial wireless is sustained by network backbones.

46 Wi-Fi, for wireless fidelity, operates on unlicensed frequencies. An example of how Wi-Fi can support public safety is the plan of Cook County, Illinois to implement Wi-Fi for public and private sector use. See “Metro Wi-Fi Finding Friends,” by Ed Sutherland, Network Computing’s Mobilepipeline, July 30, 2004 at [http://nwc.mobilepipeline.com/26100806]. Viewed February 8, 2005.
Policy and Progress

The debate about public safety communications and the role of federal policy is long running. The framework for current discussions — which accommodate recent advances in technology — most likely dates to a report in 1996 by the Public Safety Wireless Advisory Committee (PSWAC).\(^{47}\) Listed below are some key components of a desirable public safety communications policy for first responders described in the PSWAC study and in more recent reports, testimony, and other comments cited in this report. According to these sources, a national policy for public safety communications needs to address and correlate a myriad of complex goals, such as:

- Coordinated assignment and use of spectrum at various frequencies.
- Muscular and sustained efforts to complete the development and application of technical and operational standards.
- Public sector adaptation of new technologies already available in the private sector such as for high-speed, data rich, and video or image transmissions.
- Long-term support of research and development for new technology.
- Coherent goals that encourage private investment in technology development.
- Nationwide network of communications operations centers (regional signal corps) that can serve as back-up facilities to each other and to state and interstate centers and networks.
- Interoperability of communications among first responders and public safety agencies.
- Managerial structure that can successfully coordinate not only disparate federal, state and local agencies but also the different cultural and technical needs of independent first responder units.
- Framework to match policy goals with implementation needs to assure the effectiveness of federal funding for programs and grants.

Congress has responded with provisions in the National Intelligence Reform Act with specific instructions to federal departments and agencies to take actions to meet many of the goals outlined above, as well as respond to other concerns articulated by the public safety community. Key tasks that the act requires for public safety communications include

- Sense of Congress that it must pass legislation that resolves spectrum release as part of the transition to digital television; first session. Sec. 7501.

\(^{47}\) The Public Safety Wireless Advisory Committee (PSWAC) was chartered in 1995, at the request of Congress, to study public safety spectrum and make recommendations for meeting spectrum needs through the year 2010. The following year, PSWAC submitted a report containing recommendations for the improvement of public safety communications over wireless networks. *Final Report of the Public Safety Wireless Advisory Committee*, September 11, 1996.
• Requirement for a study on spectrum for public safety and homeland security; December 2005. Sec. 7502 (a).

• Requirement for a study on strategies to meet interoperable communications needs; December 2005. Sec. 7502 (b).

• Report on plan to accelerate development of national interoperable standards, including milestones and achievements; April 2005. Sec. 7303 (b).

• Establishment by the President of a mechanism for coordinating cross-border interoperability issues with Canada and Mexico; June 2006. Sec. 7303 (c).

• Requirement to establish at least two pilot projects in high threat or urban areas for interagency communications; March 2005. Sec. 7304 (a).

• Reports on interagency communications pilots; interim, June 2005; final June 2006. Sec. 7304 (e).

• Authorization of funds for interoperable communications programs; fiscal years 2005 through 2009. Sec. 7303 (a) (3).

• Requirement for a study on the use of telephone, wireless and other existing communications networks as a means of providing a nationwide emergency notification system; September 2005. Sec. 7403.

• Requirement for a pilot study using a warning system similar to the Amber Alert communications network (using funds made available for improving the national warning system regarding terrorist attacks) with a report on findings and recommendations; September 2005. Sec. 7404.

**Convergence**

The concept of public safety communications is expanding as new technology makes it possible to include many whose role in preventing or responding to disaster lies outside the conventional definition of first responder. A more inclusive description of public safety responders might include utility workers (often among the first on the scene, to shut down power sources), health care workers other than those in emergency medical services, operators in 911 call centers, and bystanders at the scene of an accident or disaster. A Focus Group for the National Reliability and Interoperability Council (NRIC VII) suggests the term “emergency agency” and provides a suggested list of “agents” that might be part of an expanded “emergency response internetwork;” “technology would provide the capability to link all parties
and policy would determine the circumstances for, and type of, communication. 48 Although not included in its list of recommendations, the 9/11 Commission commented on the often inadequate response of the 911 call centers serving New York City, 49 and suggested “In planning for future disasters, it is important to integrate those taking 911 calls into the emergency response team and to involve them in providing up-to-date information and assistance to the public.” 50 The absence of advance warning to communities inundated by tsunamis on December 6, 2004 provided a harsh reminder of the role of emergency alert systems — another form of public safety communications — in saving lives. The convergence of communications technology, typified by the near-ubiquity of the Internet and the wide availability of advanced wireless telephony, presages a world of end-to-end communications for public safety.

In a bill, enacted in the same time frame as the National Intelligence Reform Act, Congress created an E-911 Implementation Coordination Office to foster improvements in 911 call centers. 51 The National Intelligence Reform Act contains two provisions for collecting information on emergency alert systems. One requires a study about the use of telecommunications networks as part of an all-hazards warning system, specifying that technologies to consider would be “telephone, wireless communications, and other existing communications networks . . .”. 52 The act also requires a pilot study using technology now being used for an Amber Alert network, to improve public warning systems regarding threats to homeland security. This is to be conducted by the Secretary of Homeland Security in consultation with, among others, the National Association of State Chief Information Officers (NASCIO). 53 NASCIO has announced that it expects to participate actively in the pilot, expanding on Internet technology customized for Amber Alerts. 54 This alert system is managed from a dedicated Web portal that can be accessed by statewide or

---

48 NRIC VII, Focus Group 1D, Communications Issues for Emergency Communications Beyond 911; Report #1 - Properties and network architectures that communications between PSAPs and emergency services personnel must meet in the near future,” December 6, 2004, pp. 12; 26-27. PSAPs are Public Safety Answering Points, also known as 911 Call Centers. NRIC is a Federal Advisory Committee chartered by the FCC, see Appendix [http://nric.org/meetings/docs/meeting_20041206/FG1D%20Final%20Report.pdf]. Viewed February 23, 2005.


50 Op cit., p. 318.

51 P.L. 108-494, Title I.

52 Study Regarding Nationwide Emergency Notification System, National Intelligence Reform Act of 2004, Title VII, Sec. 7403.

53 Pilot Study to Move Warning Systems Into the Modern Digital Age, National Intelligence Reform Act of 2004, Title VII, Sec. 7404.

local systems. It is hoped by its developers that this system might become the backbone for an expanded all-hazards warning system that would extend the reach of emergency alerts to all types of communications media.

At present, the studies, the actions to improve federal responsiveness to public safety needs, and the goals discussed in this report are like unconnected dots on a white board. There is no mandate, for example, that the various studies requested by Congress and by the Administration be reviewed together for connecting themes or synergies, or that other reports from credible organizations — such as the Federal Advisory Committees of the FCC — be taken into account in developing new policies. Although many steps have been taken within DHS, and Congress has demanded further advances, there does not appear to be any long term strategy that takes into account both public safety spectrum needs and interoperable communications needs. Programs at SAFECOM, assigned the leading role in advancing interoperability, are primarily consultative in nature and focused on administrative issues. While SAFECOM makes important contributions to testing equipment and working on technical and operational standards for interoperable equipment, there does not appear to be a program that is intended to develop a standardized network overlay that can encompass the many useful, but unfortunately mostly not connected, networks that already play vital roles in public safety communications. Newer technologies, such as mesh networks and software-defined radio, are not required to have open platforms for public safety use. The mesh network systems being installed for public safety in some communities and cities use proprietary standards and are not interoperable, echoing the proprietary, incompatible cellular radio networks that were developed in the last century to be the mainstay of today’s mostly non-interoperable systems for public safety.

There is much still to be done to bring the United States to the threshold of achieving interoperability. Most would concur that this is a task of daunting complexity. There also appears to be a wide consensus that solutions must be found and the necessary changes made. Congress can expect that the many advocates for public safety, in all its forms, will continue to push for improvements in communications.
Appendix I - Federal Administration

The key federal agencies for spectrum management and first responder communications are the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). Among other responsibilities, the FCC supervises spectrum for non-federal public safety agency communications. The NTIA — part of the Department of Commerce — administers spectrum used by federal entities. The lead federal program for fostering interoperability is administered by the Wireless Public SAFETY Interoperable COMMunications Program, dubbed Project SAFECOM, part of the Department of Homeland Security. SAFECOM has not to date played a major role in spectrum policy. DHS has created an Office of Interoperability and Compatibility (OIC) of which SAFECOM is a part. In June 2004 DHS announced the creation of a Regional Technology Integration Initiative. DHS has also announced the organization of a National Incident Management System (NIMS) in response to a Presidential Directive (HSPD-5). A NIMS Integration Center is planned to deal with compatibility and will be responsible for at least some interoperable communications.

National Telecommunications and Information Administration

To address the need for interoperability spectrum, in June 1999 the NTIA designated certain federally-allocated radio frequencies for use by federal, state, and local law enforcement and incident response entities. The frequencies are from exclusive federal spectrum, and are adjacent to spectrum used by state and local governments. NTIA’s “interoperability plan,” — developed in coordination with the Interdepartmental Radio Advisory Committee (IRAC) — is used to improve communications in response to emergencies and threats to public safety. In 1996, the NTIA created a public safety program to coordinate federal government activities for spectrum and telecommunications related to public safety. Today, its successor, the Public Safety Division of the Office of Spectrum Management, participates in various initiatives to improve and coordinate public safety communications. The Division is preparing a Spectrum Efficiency Study and an Interoperable

55 Additional information is at [http://www.safeomprogram.gov/].

56 DHS is the managing partner for the SAFECOM program. Contributing partners include these Departments: Justice, Treasury, Transportation, Defense, Agriculture, Energy, Health and Human Services, and Interior.


58 IRAC, with representation from 20 major federal agencies, develops policies for federal spectrum use, and represents the United States at International Telecommunications Union conferences. See [http://www.ntia.doc.gov/osmhome/irac.html]. Viewed February 8, 2005.
Communications Summary Guide. 59 Two forums on public safety and spectrum use have been sponsored by the NTIA, one in June 2002 and another in February 2004. 60

Federal Communications Commission

Over roughly the last 20 years, the FCC has initiated several programs that involve state, local, tribal and — usually — private sector representatives. In 1986, it formed the National Public Safety Planning Advisory Committee to advise it on management of spectrum in the 800 MHZ band, newly designated for public safety. The following year, the FCC adopted a Public Safety National Plan that, among other things, established Regional Planning Committees (RPCs) to develop plans that met specific needs. The FCC encourages the formation of RPCs with a broad base of participation. The RPCs have flexibility in determining how best to meet state and local needs, including spectrum use and technology.

The regional planning approach is also being applied to spectrum in the Upper 700 MHz band. 61 Technical and operational standards, including interoperability standards, were developed and recommended to the FCC through the Public Safety National Coordination Committee (NCC). Standards for narrowband radio applications, for example, were recommended to the FCC and adopted in early 2001. Established by the FCC in 1999 and ended in 2003, the NCC had a Steering Committee from government, the public safety community, and the telecommunications industry.

Homeland Security. Among actions by the FCC specifically in support of homeland security were the chartering of the Media Security and Reliability Council (MSRC) 62 and the renewal of the charter for the Network Reliability and Interoperability Council (NRC). 63 Both of these are Federal Advisory Committees. MSRC has been active in evaluating the effectiveness of the Emergency Alert System. The primary role of NRIC is to develop recommendations for best practices for private sector telecommunications to insure optimal reliability, interoperability, and connectivity of networks. The current NRIC focus groups are: Near Term Issues, E911; Long Term Issues, E911; Best Practices, E911 and Public Safety; Emergency Communications Beyond E911; Best Practices, Homeland Security - Infrastructure; Best Practices, Homeland Security - CyberSecurity; Best Practices, Wireless Industry; Best Practices, Public Data Networks; and Broadband.

Spectrum and Interoperability. The FCC’s strategic goal for spectrum is to “Encourage the highest and best use of spectrum domestically and internationally


63 See [http://www.nric.org].
in order to encourage the growth and rapid deployment of innovative and efficient communications technologies and services.”

Regarding interoperability, the FCC describes its role as “directing efforts toward allocating additional spectrum for public safety systems, nurturing technological developments that enhance interoperability and providing its expertise and input for interagency efforts such as SAFECOM.” However, the FCC asserts that there are limitations on what it can do. “The Commission is only one stakeholder in the process and many of the challenges facing interoperability are a result of the disparate governmental interests . . . making it difficult to develop and deploy interoperable strategies uniformly.”

**Department of Homeland Security, Office of Interoperability and Compatibility**

The function of the Office of Interoperability and Compatibility (OIC) is to address the larger issues of interoperability. Among the goals of the OIC is the “leveraging” of “the vast range of interoperability programs and related efforts spread across the Federal Government” to “reduce unnecessary duplication” and “ensure consistency” in “research and development, testing and evaluation (RDT&E), standards, technical assistance, training, and grant funding related to interoperability.” To achieve this, DHS will create within OIC “a series of portfolios to address critical issues.” The OIC’s initial priorities are for communications (SAFECOM), equipment, training and “others as required.” To fulfill the portfolios, OIC will use a “systems engineering or lifestyle approach” to create “action plans.” These will be “developed through a collaborative process that brings together the relevant stakeholders to provide clear direction on a path forward.” This “end-user” input is expected to produce “a strategy and action plan” for each portfolio. No time line for accomplishing these planned steps has of yet been provided.

**SAFECOM.** With the support of the Administration, Project SAFECOM was designated the umbrella organization for federal support of interoperable communications. It was agreed within DHS that SAFECOM would be part of the Science and Technology Directorate, in line with a policy for placing technology prototype projects under a single directorate; this decision was reportedly based on the research-oriented nature of the programs envisioned for SAFECOM by its

---


66 Ibid.

The National Intelligence Reform Act affirmed this decision by giving DHS the authority to create an office for interoperability within the Science and Technology Directorate and to manage SAFECOM as part of that effort. SAFECOM recently released a template for interoperability planning that can be used by states to establish a strategy for interoperability and is preparing a methodology to establish a baseline for interoperability achievements as an evaluation tool to measure the success of future interoperability programs. Reportedly, SAFECOM will release initial findings on the baseline measurement some time in 2005.

SAFECOM absorbed the Public Safety Wireless Network (PSWN) Program, previously operated jointly by the Departments of Justice and the Treasury. PSWN was created to respond to recommendations made by the Public Safety Wireless Advisory Committee regarding the improvement of public safety communications over wireless networks. PSWN operated as an advocate for spectrum management policies that would improve wireless network capacity and capability for public safety. SAFECOM, however, has no authority over spectrum management decisions. The following quote is a summary of SAFECOM’s position on spectrum policy.

Spectrum policy is an essential issue in the public safety communication arena. Unfortunately, State and local public safety representatives are frequently not included in spectrum policy decisions, despite their majority ownership of the communications infrastructure and their importance as providers of public and homeland security. SAFECOM will hence play a role in representing the views of State and local stakeholders on spectrum issues within the Federal Government. Last year, SAFECOM was appointed to an interagency Spectrum Task Force to contribute such views, and the ongoing working relationship that has developed between SAFECOM and the FCC will, we believe, pay huge dividends in the future.

Regional Technology Integration Initiative

In June 2004, the Directorate of Science and Technology introduced a new initiative to facilitate the transition of innovative technologies and organizational concepts to regional, state and local authorities. The initiative has selected four
urban areas from among those currently part of the Homeland Security Urban Area Security Initiative. Two of the areas that have been reported as choices are Cincinnati, Ohio and Anaheim, California. Each area will reportedly receive $10 million to expand new systems that test more advanced technologies for public safety communications, including interoperability. Anaheim, for example, reportedly has created a virtual operations center (instead of a building), relying on network technology to connect police, fire, medical services and public utilities in case of an emergency. The announced goal is to get all who respond to disasters and other emergencies to work from a common base.

**National Incident Management System**

NIMS also has announced plans to address questions of interoperability and communications, although no mention of spectrum policy is mentioned in the DHS report on NIMS issued March 1, 2004. The objective for communications facilitation is summarized as “development and use of a common communications plan and interoperable communications processes and architectures.” NIMS envisions mandatory compliance with “national interoperable communications standards, once such standards are developed.” These standards will include interoperable wireless communications for “Federal, State, local and tribal public safety organizations.”

**Other Coordinating Bodies**

SAFECOM has created a Federal Interoperability Coordination Council (FICC), made up of “all the federal agencies with programs that address interoperability.” Previously, as part of its e-government mandate to rationalize federal programs for interoperability, SAFECOM met with representatives from 60 different programs operated by the federal government or funded by or partnered with a federal agency.

---

73 (...continued)


75 Ibid.


77 Ibid, p. 11.

78 Ibid, p. 50.

79 Ibid., p. 52.

Many of these programs include state committees and national associations such as the Association of Public-Safety Communications Officials - International (APCO).81 Part of the National Coordination Committee’s mission was to encourage the creation of Statewide Interoperability Executive Committees (SIEC),82 to take part in coordination efforts. The National Public Safety Telecommunications Council (NPSTC) is another important coordinating body. NPSTC unites public safety associations to work with federal agencies, the NCC, SIECs and other groups to address public safety communications issues.83 It has been supported by the AGILE Program, created by the National Institute of Justice (NIJ).84 AGILE has addressed interim and long-term interoperability solutions in part by testing standards for wireless telecommunications and information technology applications. The AGILE Program also has provided funding to Regional Planning Committees for start-up costs and the preparation and distribution of regional plans. AGILE is being restructured, to be replaced by a more limited function in Communications Technology, CommTech. CommTech is not designed to play a primary role in coordinating interoperability policy within the public safety community.

The SIECs, NPSTC, Regional Planning Committees and other federally-supported but not federally-directed organizations play key roles as facilitators in advancing programs for public safety communications. In recent testimony quoted above,85 both SAFECOM and the FCC have described their roles primarily as facilitators also. SAFECOM and DHS, in its plans for the Office of Interoperability and Compatibility, seem to place a high priority on consultative functions. It appears that OIC policy will focus on portfolios of recommendations for achieving interoperability at an incident site and not on establishing the higher levels of interoperability provided by network support and back-up from regional communications command centers. In its discussions of Emergency Operations Centers and Incident Command Systems, however, NIMS seems to indicate the need for a national network architecture and fixed as well as mobile operations centers for communications network support. The Regional Technology Integration Initiative has been established to act as a catalyst between existing technology used by first responders and the innovative technology needed in the future. It seeks to work at the local, state and regional levels but appears to favor solutions that can be applied on a regional basis.

In sum, although there are many worthwhile efforts and federally-funded programs for interoperability and public safety communications, it has been...

---

81 See [http://www.apcointl.org/].


83 Information at [http://npstc.du.edu/].


suggested that there does not seem to be “big picture” leadership within the federal administration. Some have suggested a public-private partnership would be more effective, including private operation of the 700 MHz spectrum that appears to be crucial to public safety’s future communications support.