Backgrounder

Published by The Heritage Foundation

No. 1951
July 17, 2006

Talking Through Disasters: The Federal Role in Emergency Communications

James Jay Carafano, Ph.D.

From September 11, 2001, to Hurricane Katrina in 2005, Congress and the Bush Administration have wrestled with the challenge of improving emergency management communications. An unprecedented federal spending spree has yielded scant progress, however, and Washington's programs should be scrapped. It is unlikely that they will ever be able to achieve, either efficiently or effectively, the goal of creating the kind of emergency communication systems the nation needs to respond to national disasters.

The right approach would include adhering to a set of policies that promote effective public–private sharing of the emergency management electromagnetic spectrum, create a national capability to deploy a wide-area emergency management communications network for catastrophic disasters, and establish coherent national leadership for emergency response communications.

What Is Being Done?

In the rush to enhance emergency management communications after 9/11, the government's solution has been to throw money at the problem, mostly through a variety of federal grants.[1] The Department of Homeland Security (DHS) has the Wireless Public Safety Interoperable Communications Program (SAFECOM), but SAFECOM has very limited authority either to oversee and coordinate federal, regional, and state efforts or to direct funding.

SAFECOM was an E-government project initiated by the Office of Management and Budget before the department was created.[2] By some estimates, SAFE-

Talking Points

- In the wake of September 11 and Hurricane Katrina, the federal government made improving emergency management communications a top legislative priority but not enough has been accomplished.
- To improve emergency responder capabilities nationwide, the government must create a system to regulate disaster site convergence by responders, improve planning, and expand the range of information that is made available to first responders.
- National standards must be established for a national response system that will enable it to respond to everyday demands, establish regional and national communications, and operate when the infrastructure is degraded.
- Frequency spectrum should be made available as "dual-use" to both commercial users and emergency responders.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/bg1951.cfm

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies of the Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

COM programs will require over 20 years and $40 billion to achieve a national interoperable emergency communications system.[3] Likewise, a proposed National Integrated Network that would bring together federal law enforcement agents from the Departments of Homeland Security, Justice, and Treasury into a single wireless infrastructure may take 15 years to build with a price tag estimated at up to $10 billion.[4]

In short, the federal government is spending a great deal of money on projects that are not well-coordinated.

Throwing money at the problem is a troubling strategy. The government's record with information technology acquisition and implementation is poor. Typically, programs lack clear requirements, as well as strong executive leadership, and underestimate the time, money, and human capital necessary to achieve what is needed. Federal efforts to promote more effective emergency management communications show little promise of doing better.

What Is Required?

Emergency responders—the millions of law enforcement, fire, medical, public services, and volunteer groups and private-sector assets that save lives and property in the aftermath of disasters—need communications that have assured:

- **Capacity** to get them the information they need to respond to both everyday missions and major disasters. That capacity must include (1) getting the right kinds of information, whether it is from other responders, agencies, jurisdictions, or levels of government; (2) obtaining information in the form they require—voice, data, or video; and (3) receiving it in a timely manner in the volumes required, whether it be through instant messaging or reams of technical data.
- **Access** to communications. Responders must have services that work in an emergency environment, whether it is rescuing injured persons underground, placing a call when phone lines are flooded with people calling 911, or accessing the Internet after a storm has wiped out power lines or an earthquake has cut underground cables.
- **Security** that responders can trust. Responders must have confidence that critical information sharing can occur without monitoring or disruption that would interfere with their ability to render assistance effectively or ensure the safety of other responders.

Most communications experts agree that there is no "silver bullet" solution that can address all these needs. They all concur, however, that the technol-

1. In a May 24, 2006, report by the Office of Grants and Training Preparedness Directorate, the Department of Homeland Security shows that from 2003 to 2005, DHS spent just over $5.6 billion on interoperable communication equipment, with $1.8 billion going toward procurement of this equipment for its interoperable communications improvement programs. See U.S. Department of Homeland Security, Office of Grants Training Preparedness Directorate, "Interoperable Communications Technical Assistance Program," May 24, 2006, at *www.search.org/conferences/2006interop/agenda/presentations/Keith%20Young%20-%20DOJCOPS-AUSTIN.ppt#326* (June 26, 2006). In addition, the Deficit Reduction Act of 2005 (DRA) created new grant programs, including $1 billion to assist public safety agencies in the acquisition, deployment, or training for the use of interoperable communications systems, to be administered by the National Telecommunications and Information Administration (NTIA) but requiring the NTIA to consult with DHS in its implementation of the program. For a copy of the DRA, see "Deficit Reduction Act of 2005," S. 1932, January 3, 2006, at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:s1932enr.txt.pdf* (June 26, 2006).
2. U.S. Government Accountability Office, *Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders*, GAO–04–1057T, September 2004, at *www.gao.gov/highlights/d041057thigh.pdf* (June 16, 2006).
3. David Boyd, "SAFECOM: Improving Public Safety Wireless Communications and Interoperability," March 17, 2004, p. 12, at *www.interoperability.publicsafety.virginia.gov/Library/PDFs/SAFECOM-ImprovingWirelessComms.pdf*, and Karen D. Schwartz, "Straight Talk," *Government Executive*, October 1, 2004, at *www.govexec.com/features/1004-01/1004-01managetech.htm* (July 11, 2005).
4. Alice Lipowicz, "Hurricanes a Boost for Integrated Wireless Networks," *Washington Technology*, Vol. 20, No. 24 (December 12, 2005), at *www.washingtontechnology.com/news/20_24/federal/27577-1.html* (June 16, 2006).

ogies needed to provide the right services exist today. Commercial off-the-shelf technologies, such as cellular service, video-streaming, and Voice-over-Internet-Protocol (VoIP), are robust and mature. The challenge is applying them to the needs of responders.

What Is the Priority?

Enormous confusion persists about what Washington should be doing to support the establishment of more effective communications for the nation's responders. The simplistic and often-repeated mantra that responders need "interoperable" communications fails to describe the real requirements.[5] A better approach is needed.

Congress and the Bush Administration are right to focus on the communications requirements of responders, but they first need to understand the real needs in order to foster useful and affordable solutions. There are three significant challenges that present themselves in almost every large-scale disaster:[6]

- **Convergence.** The most common problem at a disaster is too much—not too little—aid. In disasters, public and private responders tend to converge on a disaster, choking the scene with people, equipment, and supplies that create security and safety risks, logistical nightmares, and confusion that hinders the delivery of help.
- **Lack of interagency planning.** Plans fail not because responders have not planned how to respond, but because they have failed to coordinate and exercise their plans with one another. This problem persists both within jurisdictions and across levels of government and the private sector.
- **Lack of information.** Knowing the location and nature of threats (natural or man-made), victims, responders, and available assets, as well as conditions in the area, can be extremely difficult. The press for time, chaos, stress, and the inability to deliver vast amounts of data in a usable form can all make the problem of dealing with disasters much worse.

Effective communications can be of significant help in addressing all of these issues by getting the right information to the right person at the right time.

Interoperable radios are one means by which to share information, but they are not always the best, the most efficient, or the most effective. Not all responders need to talk to each other. In fact, having too many users (fire *and* police, for example) sharing a communications network can overload a system, slowing coordination or sowing confusion. Pursuing interoperability as an end in itself is a bad strategy, as is spending vast amounts of money on capabilities that are not essential, not appropriate, or perhaps not even needed.

Addressing the most serious problems requires more sophisticated solutions than simply demanding vast amounts of federal tax dollars for interoperable communications, and deciding how the federal government can best address communications shortfalls requires understanding Washington's proper role. Responding to emergencies is primarily a state and local government mission.[7]

The federal government should therefore focus on the tasks that only Washington can perform. Only the federal government can integrate the efforts of local, state, regional, and private-sector assets into a national response system that enables the nation as a whole to support local communities in the event of a

5. Interoperable communications are those that involve "the ability of public safety agencies to talk to one another via radio communications systems to exchange voice and/or data with one another on demand, in real-time, when needed." National Task Force on Interoperability, *Why Can't We Talk? Working Together to Bridge the Communications Gap to Save Lives: A Guide for Public Officials*, February 2003, p. 5, at *www.safecomprogram.gov/NR/rdonlyres/322B4367-265C-45FB-8EEA-BD0FEBDA95A8/0/Why_cant_we_talk_NTFI_Guide.pdf* (July 11, 2006).
6. Mark Sauter and James Jay Carafano, *Homeland Security: A Complete Guide to Understanding, Preventing, and Surviving Terrorism* (New York: McGraw Hill, 2005), pp. 308–309.
7. James Jay Carafano, "Improving the National Response to Catastrophic Disaster," testimony before the Committee on Government Reform, U.S. House of Representatives, September 15, 2005, at *www.heritage.org/Research/HomelandDefense/tst091505a.cfm* (July 11, 2006).

disaster. It is Washington's job to ensure the means and capacity for all jurisdictions to "plug" into a national system. Additionally, the federal government should concentrate on responding to catastrophic disasters that put tens of thousands of lives and billions of dollars in property at risk—dangers that would overwhelm the capacity of any state or local government.

With regard to emergency management communications, creating a national response network and responding to catastrophic disasters should define where Washington puts its priority effort. There are three aspects to emergency management communications:

- **Responding** to everyday demands (the fires, criminal acts, and accidents that happen in communities routinely);
- **Establishing** regional and national communications so that local, state, and federal public and private assets can be coordinated; and
- **Operating** under severe conditions when infrastructure is degraded (a widespread blackout, for example) or overwhelmed by a surge in demand (such as when the New York 911 system crashed after the World Trade Center collapsed).

Clearly, Washington should focus on the second two, which are consistent with the federal mandate of creating a national system and responding to catastrophic disasters.

What Are the Best Policies?

Federal emergency management communications effort should be focused exclusively on the highest federal priorities—building the capacity for jurisdictions across the country to share critical information, act in a collaborative manner, and operate even when normal telecommunications systems are wiped out or overwhelmed.

Even with the right priorities, however, it will be difficult for the federal government to enhance the role it plays unless it adopts policies that address the major obstacles to building better capabilities. These policies include the following.

Policy #1: Put First Things First

Wireless communications will form the backbone of any emergency communications system. In a wireless system, information is transmitted over parts of the electromagnetic spectrum rather than through wire lines or cables. This is important because in a disaster, infrastructure such as phone lines or switching trunks might be disrupted.

Additionally, responders may need information in places where there are no fixed communications systems available. In these cases, the federal government plays a significant role. The electromagnetic spectrum that carries wireless communications is managed by the federal government. Some is auctioned for commercial use. Other spectrum is allocated for public purposes. Current federal policies do not facilitate creating a national emergency network or building the capacity for responding to catastrophic disasters.

Federal, state, and local public safety agencies already have a large allocation of spectrum for emergency responders. The problem is that the allocation is scattered throughout the frequency band, which is grossly inefficient. Compared to the commercial use of the spectrum, emergency response networks carry a much smaller number of transactions with only an intermittent surge in demand. As a result, bandwidth is significantly underutilized.

In turn, local jurisdictions manage their spectrum by breaking allocations into smaller pools of channels for each individual agency (such as giving fire departments in neighboring communities their own dedicated channels). Further splitting the spectrum exacerbates the inefficiency of underutilization. In many cases, federal, state, and local responders do not even have the capacity to share spectrum when they are all working in the same region and responding to the same crisis.[8]

8. Although the FCC has provided 50 MHz in the 4.9GHz band for public safety broadband applications, this spectrum is primarily suited for "hot spot," on-scene communications. It is not viable to support wide-area communications because of its limited propagation characteristics. Public safety also has an allocation of 24 MHz for voice and wide-band applications in the 700 MHz band, but it is not allocated to support more advanced, mobile broadband/voice-over-Internet capabilities.

The commercial space uses the spectrum about 20 times more efficiently than governments use it.[9] The spectrum licensed to federal, state, and local public safety users supports fewer than 3 million users across the U.S. In contrast, commercial operators (such as Sprint and T-Mobile) support about 80 million users in a comparable amount of spectrum. Additionally, the commercial networks provide both voice and high-speed data. Most public safety networks carry voice service only.

With a relatively small number of users, the emergency management spectrum holds little attraction for private-sector service providers. There is virtually no incentive for private-sector investment. Economies of scale cannot be used to spur investments, to innovate, and to reduce costs. However, that could change if federal policies created commercial opportunities.

Policy #2: Open Emergency Management Frequencies as Dual-Use Spectrum

The government should provide the private sector with opportunities to offer commercial services in bandwidth that currently is reserved for public safety agencies. In turn, the private sector could invest in building up capacity for emergency services to operate within the spectrum and provide state-of-the-art, low-cost, secure services and guaranteed access during disaster situations. Prohibitions against sharing the public safety spectrum should be eliminated, and federal agencies should have greater flexibility in deciding how to share, sell, or barter spectrum to obtain the emergency communications services they need from the private sector.

Legacy Investments. Even if responders shared spectrum with the private sector, this would not completely solve the problem. For decades, public safety agencies have deployed a plethora of technologies, much of them outdated compared to what is commercially available. Many public safety agencies have technology that is so old that it is not compatible with commercial systems.

In part, the public safety spectrum is organized to accommodate the older, narrow-band technologies. This means that the frequencies available for emergency services cannot support high-speed data transmissions like streaming video, VoIP, or large amounts of digital data such as building floor plans, information on dealing with hazardous materials, or various kinds of geospatial data like traffic and wind patterns.

While the responders' legacy systems have shortcomings, it is unrealistic to believe that these systems can be scrapped wholesale, with the federal government paying equipment, training, and replacement costs. By some estimates, there are over 44,000 local and state agencies that each have their own unique systems and requirements.[10]

Policy #3: Don't Send Money; Set Standards

Rather than trying to fix the problem, the federal government's first priority should be to keep it from getting worse. National standards should be set that would migrate systems over time into a common, open architecture that is compatible with industry standards and could utilize commercial off-the-shelf technologies to provide responders with state-of-the-art systems. These would enable responders to talk to one another, utilizing the kind of bandwidth necessary for robust communications.

For example, the problems hindering voice interoperability could be addressed as agencies procured networks built on a common IP-based standard. IP-based systems would allow interoperability across multiple agencies, jurisdictions, and geographic areas, as well as with commercial, cellular-based networks, eliminating the need to build expensive, dedicated, private proprietary networks.

In addition to standards for communications systems, standards must be established for the recovery and reconstitution of critical infrastructure that supports these networks. This should extend to assets that support critical risk communications for average citizens, such as public warning systems and emergency services like 911.

9. See Gerald R. Faulhaber and David Faber, "Spectrum Management: Property Rights and the Commons," undated, at *http://assets.wharton.upenn.edu/~faulhabe/SPECTRUM_MANAGEMENTv51.pdf* (July 12, 2006).
10. David G. Boyd, testimony before the Committee on Government Reform, U.S. House of Representatives, November 6, 2003, at *http://reform.house.gov/UploadedFiles/Boyd%20SAFECOM%20testimony.pdf* (June 16, 2006).

Land-Based Systems. Current public safety networks are based primarily on mobile, land-based communications, such as the radios in police cars and fire trucks. In turn, these report to fixed, land-based sites such as police stations and emergency operations centers. These networks often prove inadequate to support robust responses to large-scale disasters. They are optimized for voice communications, lacking the capacity to exploit cutting-edge technologies like broadband services. Emergency service networks also have limited power and range. Ground-based signals can be masked by high buildings, underground subways, and terrain features such as hills and forests.

Additionally, ground-based signals are vulnerable. The aftermath of Hurricane Katrina offers numerous examples of flooding that wiped out roads, cell towers, and fire stations, or of communications that went out because generators ran out of fuel or radios lacked fresh batteries. The attack on the World Trade Center destroyed New York City's emergency operations center. Overall, land-based systems are inadequate to "scale-up" to meeting the needs of responding to catastrophic disasters.

On the other hand, non–terrestrially based systems remain highly resilient in the face of disasters. This proved particularly true in the aftermath of Katrina. Satellite-based systems and pagers remained dependable despite the devastation.

There needs to be a supplement to the land-based systems used by local emergency responders, particularly for large-scale disasters that cover a wide area and require jurisdictions to coordinate their activities when much of the supporting infrastructure may be destroyed or unusable. This system should be non–territorially based, using either air or spaceborne platforms, or a combination of both. Here, it is appropriate for the federal government to step up and provide the capability to establish an emergency *ad hoc*, wide-area wireless network to support both existing (voice radio) and emerging (VoIP, geospatial data, and video) capabilities.

Policy #4: Buy Services, Not Infrastructure or Technology

Rather than attempting to develop and deploy a communications architecture along with all the hardware (e.g., planes, unmanned aerial vehicles, aerostats, or satellites) and software, the federal government should buy the services it needs from the private sector. In addition, Washington should not specify particular technological solutions. Government should specify performance needs and let the private sector figure out how to best meet the challenge. This will provide cheaper capabilities sooner and allow agencies to upgrade quickly as the commercial sector brings new products and services online.

Who Should Lead?

There is too much federal leadership in disaster emergency management communications. The National Telecommunications and Information Administration manages the spectrum for use by federal agencies. The Federal Communications Commission, however, manages other spectrum allocations and recently established a Public Safety and Homeland Security Bureau to address public safety, homeland security, national security, emergency management and preparedness, and disaster management issues.

In addition, DHS allocates homeland security grants and houses the office that administers SAFECOM and the National Communications System, which is responsible for the federal emergency communications system. The Departments of Justice and Treasury, along with DHS, are responsible for administering the National Integrated Network. Other federal departments, including the Departments of Defense and Interior, also have equities in domestic emergency communications management planning.

In other words, a lot of federal stakeholders are at the table, and all of these agencies have important roles to play. Yet the current organization of federal activities has proved unsatisfactory.[11] It is unrealistic to give all the responsibility to one agency or to put it in charge of an unwieldy interagency effort. A more organized effort is necessary.

Policy #5: Match Missions and Resources to Priorities

Congress should establish legislative mandates for specific federal agencies to perform specific

tasks, setting clear deliverables and reasonable milestones for their achievement. Legislation not only would serve as a contract between leaders in Congress and the Bush Administration on the way forward, but also would act as a guide to congressional appropriators, ensuring that budget priorities match the priority of effort. The various offices and programs within DHS that are responsible for assorted aspects of communications planning need to be aligned under the appropriate authority in the department (e.g., the Undersecretaries for Preparedness and Science and Technology and the Director of Operations Coordination).

Road Map to the Future

If Congress and the Bush Administration are serious about improving the emergency responder capabilities nationwide, they need to put these principles into practice. That will require:

- **Scaling** back bloated, bureaucratic programs and wasteful homeland security and interoperability grants;
- **Focusing** on developing capabilities to enhance regional information sharing and response to catastrophic disasters;
- **Revising** federal policies and laws to open dual-use spectrum for commercial and emergency management use, as well as facilitating the sharing of spectrum among local, state, and federal users;
- **Setting** national standards to promote open-architecture, non-proprietary systems that are compatible with commercial standards;
- **Establishing** services that can provide an emergency wide-area network wireless system to support existing responder communications equipment and emerging capabilities like VoIP; and
- **Assigning** specific missions and responsibilities to agencies for the implementation of critical policies.

Taking these steps now will meet the nation's short-term needs for building a truly national responder network that can deal with large-scale disasters. It will also establish the foundation for long-term solutions that can exploit the communications revolution that is occurring in the marketplace.

—James Jay Carafano, Ph.D., is Senior Research Fellow for National Security and Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. The author would like to thank James L. Gattuso, Senior Research Fellow in Regulatory Policy in the Thomas A. Roe Institute for Economic Policy Studies at The Heritage Foundation, and Laura P. Keith, a Research Assistant in the Allison Center, for their assistance with this paper.

11. Homeland Security Presidential Directive–3 (HSPD–3) outlined a "Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people." See George W. Bush, "Homeland Security Presidential Directive–3," March 11, 2003, at *www.whitehouse.gov/news/releases/2002/03/20020312-5.html* (July 11, 2006). HSPD–5 directed DHS to create a National Incident Management System (NIMS) to provide for "interoperability and compatibility" at all state and local levels, including communications and information systems for a common operating picture. See George W. Bush, "Homeland Security Presidential Directive/HSPD–5," February 28, 2003, at *www.whitehouse.gov/news/releases/2003/02/20030228-9.html* (July 11, 2006). The directives and their subsequent NIMS do not clearly define either the state, local, and federal roles or problems surrounding public safety communication.