United States Government Accountability Office

GAO

Report to the Chairman, Subcommittee on Communications, Technology, and the Internet, Committee on Commerce, Science & Transportation, United States Senate

June 2009

EMERGENCY COMMUNICATIONS

Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts

GAO

Accountability * Integrity * Reliability

GAO-09-604

June 2009

EMERGENCY COMMUNICATIONS

Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-604, a report to the Chairman, Subcommittee on Communications, Technology, and the Internet, Committee on Commerce, Science & Transportation, United States Senate

Why GAO Did This Study

Emergency communications breakdowns undermined response efforts during terrorist attacks in 2001 and Hurricane Katrina in 2005. In response, federal agencies like the Department of Homeland Security (DHS) and Federal Communications Commission (FCC) have increased efforts to enhance emergency communications. This requested report identifies (1) vulnerabilities, if any, to emergency communications systems; (2) federal assistance available or planned to first responders for addressing vulnerabilities or enhancing emergency communications; and (3) challenges, if any, with federal emergency communications efforts. GAO developed six catastrophic disaster case studies, reviewed agency documents, and interviewed public and private sector officials at the national, state, and local levels.

What GAO Recommends

GAO recommends that DHS complete efforts to help implement the National Emergency Communications Plan; DHS and FCC establish a forum or other mechanism to collaborate on significant agency emergency communications efforts; and DHS leverage its expertise to help federal agencies develop emergency communications plans. DHS and FCC generally agreed with the recommendations. FCC raised concerns about the report's depth and scope. GAO clarified the scope and made other changes, as appropriate.

View GAO-09-604 or key components.

For more information, contact David J. Wise at (202) 512-2834 or wised@gao.gov.

What GAO Found

Continuity of communications, capacity, and interoperability are primary areas of vulnerability in first responder emergency communications in communities across the country. The destructive nature of catastrophic disasters can disrupt continuity of communications—the ability to maintain communications during and following a disaster. A volcanic mudflow at Mount Rainier, Washington, could destroy infrastructure supporting communications systems. Capacity—a communication system's ability to handle demand, provide coverage, and send different types of information—is also vulnerable in a catastrophic disaster. For example, blind spots, areas outside the range of communications systems, could inhibit response. Lastly, vulnerabilities involving interoperability—the ability to communicate across different organizations and jurisdictions as needed and authorized—remain due to technological and human factors.

Federal agencies provide a wide range of assistance intended to help first responders mitigate emergency communications vulnerabilities. GAO grouped available federal assistance into three categories: (1) new guidance and other significant federal efforts; (2) grants and funding; and (3) technical support and federal assets. DHS and other federal agencies have taken strategic steps to enhance emergency communications by issuing key documents like the National Emergency Communications Plan—the first strategic document for improving emergency communications nationwide. Numerous grants are available and are increasingly aligned with recently developed national and state plans. Federal agencies like DHS also offer technical support intended to help mitigate vulnerabilities through planning and on-the-scene assistance.

Limited collaboration and monitoring jeopardize federal emergency communications efforts, even as the federal government has taken strategic steps to assist first responders. Federal agencies have demonstrated limited use of some best practices that GAO previously reported as helpful for addressing issues like emergency communications. Delays in establishing the Emergency Communications Preparedness Center, which would help define common goals and mutually reinforcing strategies—two collaboration best practices—undermine the National Emergency Communications Plan's implementation. DHS and FCC have also not applied these practices in FCC's effort to promote a public safety network for emergency communications. Agency officials reported it was either too early or not the agency's responsibility to use these best practices in developing this network. DHS did not submit formal comments to FCC and FCC officials described its proposed network as separate from DHS emergency communications efforts. However, GAO found potential opportunities to align these agencies' efforts. Another collaboration best practice is leveraging resources, which DHS has done in providing emergency communications technical assistance and planning guidance. But efforts have focused on state and local jurisdictions and less on federal agencies, some of which lack formal emergency communications plans. Monitoring is also crucial in helping agencies meet goals.

Contents

Letter 1

Results in Brief 4
Background 8
Continuity of Communications, Capacity, and Interoperability Are Primary Areas Where Emergency Communications Remain Vulnerable 15
Catastrophic Disasters Threaten Continuity of Communications 15
Limited System Capacity Hinders First Responders' Communications 21
Interoperability Vulnerabilities Persist 25
A Wide Range of Federal Assistance Aimed at Helping First Responders Mitigate Emergency Communications Vulnerabilities 29
New Strategic Guidance among Significant Federal Efforts to Enhance Emergency Communications 29
A Variety of Federal Funding Available 34
Technical Support and Federal Assets Are Intended to Help Mitigate Emergency Communications Vulnerabilities 38
Limited Collaboration and Monitoring Jeopardize Significant Federal Efforts and Impede Progress 42
Conclusions 60
Recommendations for Executive Action 61
Agency Comments 62

Appendix I **Objectives, Scope, and Methodology** 67

Appendix II **Case Study Disaster Scenarios** 72

Sacramento Flooding 72
Miami Hurricane 74
Honolulu/Hilo Tsunami 77
Boston Terrorist Attack 80
Memphis Earthquake 82
Mount Rainier Volcanic Mudflow 85

Appendix III **Descriptions of Communications Systems and Technologies Used by First Responders** 88

Appendix IV **Stakeholder Group and Advisory Committee Descriptions** 92

Appendix V **Comments from the Department of Homeland Security** 93

Appendix VI **Comments from the Department of Commerce** 95

Appendix VII **Comments from the Department of the Interior** 96

Appendix VIII **GAO Contact and Staff Acknowledgments** 97

Tables

Table 1: Best Practices in Collaboration 14
Table 2: 700 MHz Public/Private Partnership Proceeding 32
Table 3: DHS Command, Control and Interoperability Division - identified Challenges to FCC's 700 MHz Public/Private Partnership 48
Table 4: DHS Stakeholder Groups and Tracking Activities 58

Figures

Figure 1: Emergency Communications Case Study Locations and Disaster Type 3
Figure 2: Examples of Natural Disaster Hazards in the United States 9
Figure 3: Upper 700 MHz D Block and Public Safety Broadband Allocation 13
Figure 4: Vulnerabilities Involving Continuity of Communications in an Earthquake Scenario 16
Figure 5: Exposed, Hanging Cable at Mount Rainier National Park 18
Figure 6: Vulnerable Fuel Tank in the New Madrid Seismic Zone 19
Figure 7: Vulnerabilities Involving Capacity Limitations in a Lahar—Volcanic Mudflow—Scenario 21

Figure 8: Jurisdictions' Emergency Response Vehicles 24
Figure 9: Vulnerabilities Involving Interoperability in a Hurricane Scenario 26
Figure 10: National Emergency Communications Plan Framework 30
Figure 11: Status of Regional Emergency Communications Coordination Working Groups 34
Figure 12: Public Safety Interoperable Communications Grants and Efforts to Align Targeted Investments for First Responders with the SCIP 38
Figure 13: FEMA Mobile Emergency Response Support Vehicle 42
Figure 14: Analysis of FCC's Third Further Notice and DHS Efforts 52
Figure 15: Analysis of Advisory Group Recommendations 2004-2008 57
Figure 16: Number of Major Flood Declarations by County, 1980 - 2005 74
Figure 17: Number of Hurricane Strikes by County, 1980 - 2007 76
Figure 18: Tsunami Hazard Based on Frequency 79
Figure 19: Urban Areas Security Initiative Regions, 2008 82
Figure 20: High, Medium, and Low Seismic Hazards 85
Figure 21: Location of High Threat and Very High Threat Volcanoes in the United States 87
Figure 22: Depiction of Land Mobile Radio System 89

Abbreviations

DHS	Department of Homeland Security
DOJ	Department of Justice
FCC	Federal Communications Commission
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
MOU	memorandum of understanding
NOAA	National Oceanic and Atmospheric Administration
NCS	National Communications System
NTIA	National Telecommunications and Information Administration
SCIP	Statewide Communications Interoperability Plan
USGS	United States Geological Survey

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

June 26, 2009

The Honorable John F. Kerry
Chairman
Subcommittee on Communications,
Technology, and the Internet
Committee on Commerce,
Science & Transportation
United States Senate

Dear Mr. Chairman:

The September 11, 2001, terrorist attacks and response to Hurricane Katrina in 2005 exposed the severe consequences of breakdowns in emergency communications used by first responders. Failures in emergency communications resulted in numerous lost lives and exacerbated already challenging situations. These past events have increased focus on the need to enhance emergency communications to respond more effectively to future catastrophic disasters. Effective response to catastrophic disasters will require that first responders—law enforcement personnel, firefighters, and others first on the scene—have reliable communication systems, including supporting infrastructure, facilities, and staff. Such communication systems would enable first responders to communicate through voice, video, and other information seamlessly among themselves, various organizations, and different levels of government. Unless otherwise noted, when we refer to emergency communications systems, we mean those systems used by first responders. Since September 11, 2001, state and local jurisdictions, as well as the private sector, have invested billions of dollars to build and enhance existing communications systems.

Federal agencies have played and will continue to play an important role in supporting the further enhancement of emergency communications. The Department of Homeland Security (DHS) has led the development of guidance and equipment standards, as well as technological innovation. The Federal Emergency Management Agency (FEMA) within DHS has distributed grant funding, maintained and provided emergency communications assets, and developed assessment and planning tools for state and local jurisdictions. Other federal agency efforts are also underway. The Federal Communications Commission (FCC), an independent regulatory agency that oversees use of radio spectrum for non-federal entities, is currently pursuing the development of a nationwide, interoperable broadband network for public safety. Because

catastrophic disasters can almost immediately overwhelm the response capabilities of state and local first responders, effective federal support before, during, and after such a disaster will be critical. That support may include providing communication assets, personnel, and support directly to state and local first responders. We have previously reported that best practices in collaboration and monitoring can aid federal agencies in addressing national, cross-cutting issues such as emergency communications.[1] In particular, we have found that given the importance of emergency communications and limited resources, it is critical that agencies find ways to work together to achieve effective and efficient outcomes.

In response to your request, this report focuses on issues related to emergency communications systems used by first responders in the aftermath of catastrophic disasters. Specifically, we identified and examined (1) vulnerabilities, if any, to emergency communications systems, (2) federal assistance available or planned to first responders for addressing any vulnerabilities or enhancing emergency communications, and (3) challenges, if any, with federal emergency communications efforts.

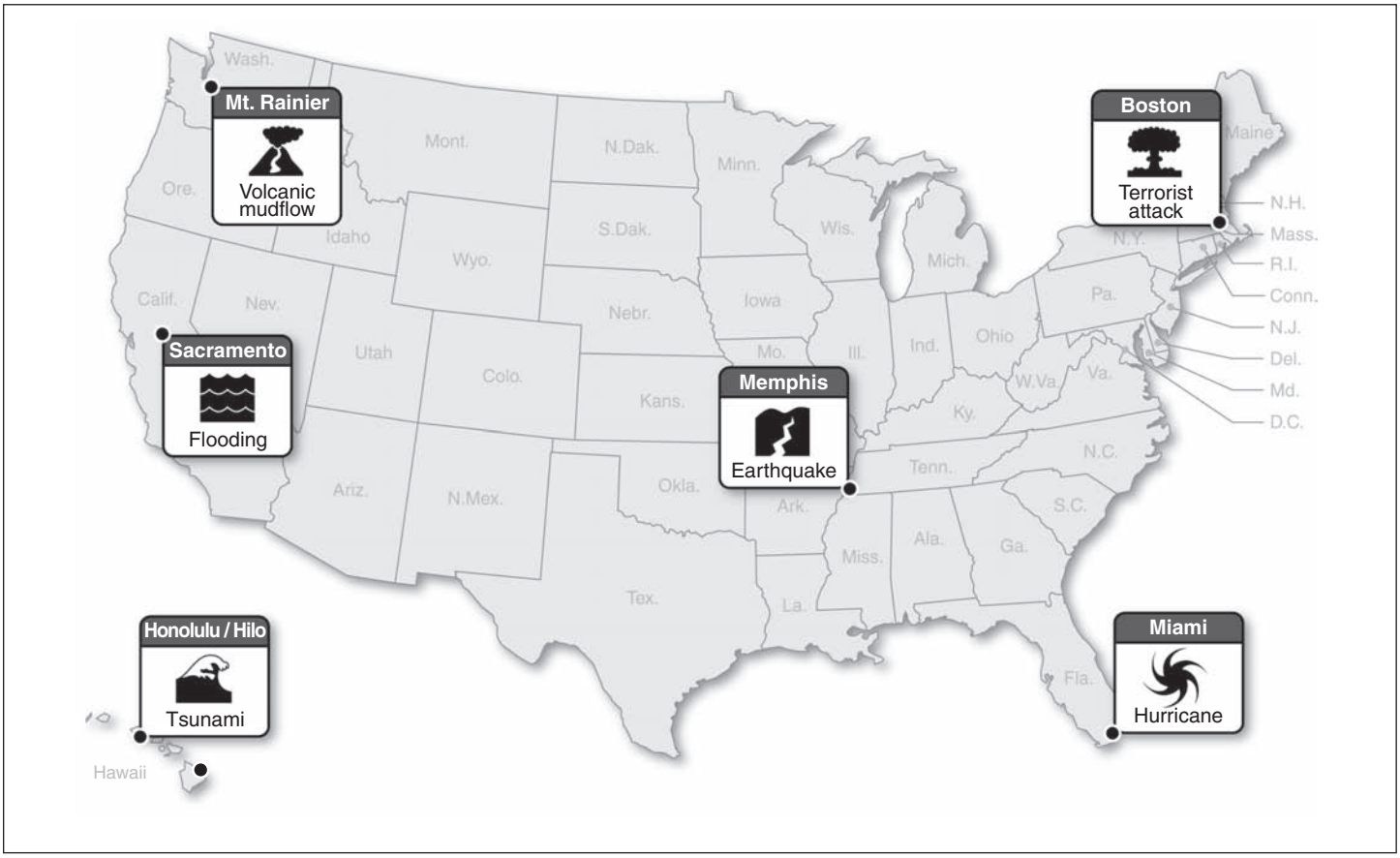
To identify and examine vulnerabilities, if any, to existing emergency communications systems, we developed six case studies and subsequent analyses of varying catastrophic disaster scenarios both natural and man-made (see fig. 1). These case studies included a flood in northern California, a hurricane in southern Florida, a tsunami in Hawaii, a terrorist attack in Massachusetts, an earthquake in Tennessee, and a volcanic mudflow in the state of Washington. In selecting our case studies involving natural disasters, we conferred with subject matter experts from the National Oceanic and Atmospheric Administration (NOAA), United States Geological Survey (USGS), and other nongovernmental entities, as well as reviewed data on each respective location's natural hazards. We also considered factors such as the likelihood of occurrence, economic impacts, potential fatalities and injuries, and geographic diversity. For our case study involving a terrorist attack, we used scenario information produced by the Homeland Security Council[2] and selected a New England

[1]See GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005); and *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996).

[2]Homeland Security Council, *Planning Scenarios – Executive Summaries*, Version 2.0 (Washington, D.C.: July 2004).

location to provide geographic diversity among our six case studies. We visited site locations for each of our six case studies and interviewed local and state emergency managers; police officers, firefighters, and other first responders; and regional federal officials to help identify emergency communications vulnerabilities. We also conducted a literature review of our prior products and other federal agency reports on emergency communications to analyze and ascertain common vulnerabilities.

Figure 1: Emergency Communications Case Study Locations and Disaster Type



Sources: GAO and MapArt.

To identify and examine federal assistance available to first responders for emergency communications, we interviewed officials and reviewed program documents from a variety of federal agencies with responsibility for emergency communications efforts available or planned, such as DHS, FCC, and the Department of Justice (DOJ). During our case study work,

state and local first responders, as well as federal officials, also provided information on federal efforts that we report on. To identify and examine any challenges in the federal approach to supporting emergency communications, we consulted our related past work on emergency communications, interagency collaboration, and federal government program management and performance. We analyzed key federal agency documents, such as DHS's National Emergency Communications Plan and FCC's notices for proposed rulemaking for an interoperable nationwide broadband public safety network to determine the extent of interagency collaboration and monitoring in some significant federal efforts. We interviewed federal agency officials to determine what steps had been taken by their respective agencies to collaborate and monitor these efforts. We also interviewed state and local first responders, professional and trade group representatives, and officials in the telecommunications industry to obtain their perspectives on significant federal efforts.

We conducted this performance audit work from February 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

Continuity of communications, capacity, and interoperability are the primary areas of vulnerability in emergency communications that persist in communities across the country, based on interviews with state and local first responders in our six case studies and others, as well as a literature review, including our prior work. DHS and FCC have described similar vulnerabilities. First responders also noted that communications vulnerabilities extend beyond our case study locations and disaster scenarios.

- Through powerful effects, such as high winds and ground shaking, potential catastrophic disasters can disrupt continuity of communications—the ability to maintain communications during and following a disaster—by destroying infrastructure supporting communications systems. For example, a volcanic mudflow at Mount Rainier National Park in Washington state could destroy cable supporting phone communications. In addition, disasters may limit continuity of communications by damaging communications facilities and stranding first responders. For example, a major earthquake in Tennessee could

damage roads and bridges, stranding Memphis first responders across the Mississippi River.

- Limitations in system capacity—a communication system's ability to handle demand, provide coverage, and send different types of information—could inhibit response. Spikes in demand following a disaster can cause communications systems to crash and system outages place additional demands on remaining systems. In addition, areas outside of the range of local communications systems can limit response efforts by creating "blind spots" in coverage, such as those found in Hawaii's mountainous terrain. Furthermore, some equipment may lack the capacity to send photographs and video, reducing first responders' situational awareness.
- We have previously reported on vulnerabilities involving interoperability—the ability to communicate across different organizations and jurisdictions as needed and authorized—and first responders we interviewed identified technological and human factors that continue to limit interoperability. Jurisdictions use various, and at times incompatible, communications systems. For example, some fire departments have hesitated to use digital radio systems, which could create incompatibility with other first responder systems, such as law enforcement. The fast-changing nature of technology compounds the difficulty of fostering and maintaining interoperability. Human factors can also limit interoperability, such as the increasingly critical need to have staff trained to coordinate with a growing number of jurisdictions.

Federal agencies provide a wide range of assistance intended to help first responders mitigate emergency communications vulnerabilities, which we grouped in three categories: (1) new guidance and other significant federal efforts, (2) grants and funding, and (3) technical support and federal assets. Recently, DHS and other federal agencies have taken significant and strategic steps to enhance emergency communications by issuing the National Emergency Communications Plan in July 2008, the first strategic document focused exclusively on improving emergency communications nationwide. Other recent federal efforts underway include completing a memorandum of understanding (MOU) to establish the Emergency Communications Preparedness Center—to be jointly operated by a number of federal agencies such as DHS, FCC, and the Department of Commerce, as the focal point and clearinghouse for implementing federal interoperability efforts—and establishing multiple DHS and FCC stakeholder groups to formulate recommendations for improving emergency communications based on lessons learned from previous disasters. The second category of assistance includes a wide range of grants and funding, some of which are increasingly aligned with recently developed national and state plans. Finally, federal agencies such as DHS

offer technical support and assets intended to help mitigate emergency communications vulnerabilities, both through advanced planning and on-the-scene assistance. For example, DHS has developed programs such as the Interoperable Communications Technical Assistance Program, providing support to first responders for planning and technical issues to be considered when developing interoperable communications.

Limited collaboration and monitoring jeopardize progress in emergency communications, even as the federal government has taken significant and strategic steps to assist first responders. Federal agencies have demonstrated limited application of some collaboration best practices that we have previously reported as helping address issues like emergency communications, which are national in scope and cross agency jurisdictions. For example, delays in establishing the Emergency Communications Preparedness Center, which would help define common goals and mutually reinforcing strategies—two collaboration best practices—undermine the implementation of the National Emergency Communications Plan, which relies heavily on participation from multiple agencies. Additionally, DHS and FCC have not established a common vision or mutually reinforcing strategies for a nationwide broadband public safety policy, although both agencies play key roles in such a development—DHS as the agency responsible for developing and overseeing the National Emergency Communications Plan and FCC as the agency charged with overseeing spectrum for non-federal entities. Although FCC has for the last several years been engaged in an effort to promote a nationwide interoperable broadband network for public safety ("700 MHz Public/Private Partnership"), there has been limited coordination with DHS. According to officials from DHS and FCC, it was either too early or not the agency's responsibility to undertake these best practices for this effort. DHS did not submit formal comments to FCC during its most recent 700 MHz Public/Private Partnership comment period. FCC officials described the 700 MHz Public/Private Partnership and the National Emergency Communications Plan as two separate, but parallel efforts. However, based on our analysis, we found potential opportunities to align DHS and FCC emergency communications efforts. Another collaboration best practice is leveraging resources. While DHS has leveraged its expertise in emergency communications planning to provide technical assistance and guidance, these efforts have focused on state and local jurisdictions, and less so on other federal agencies, some of which do not have formal emergency communications plans. We have also previously reported that monitoring and evaluating efforts are crucial elements to achieving agency goals. Although DHS and FCC have various ways of examining stakeholder group recommendations, neither agency

systematically monitors or evaluates recommendations from agency-assembled stakeholder groups or the agency's response either, potentially limiting the groups' relevance and value in addressing vulnerabilities.

We make four recommendations in this report to improve federal agencies' collaboration and monitoring in efforts related to emergency communications. To help foster implementation of the National Emergency Communications Plan, we are recommending that the Secretary of Homeland Security work to complete a memorandum to establish the Emergency Communications Preparedness Center. To help ensure that significant federal efforts are collaborative, we are recommending that the Secretary of Homeland Security and the Chair of FCC establish a forum, or other mechanism, to better collaborate to identify and discuss challenges, opportunities, and potential ways to better align their emergency communications efforts, such as the National Emergency Communications Plan and the 700 MHz Public/Private Partnership. To help ensure that federal agencies are well-positioned to support state and local first responders in a disaster, we are recommending that the Secretary of Homeland Security provide guidance and technical assistance to federal agencies in developing formal emergency communications plans. Finally, to enhance the value of DHS and FCC stakeholder group recommendations, we are recommending that the Secretary of Homeland Security and the Chair of FCC systematically track, assess, and respond to stakeholder groups' recommendations.

We provided a draft of this report, for official review and comment, to DHS, FCC, Commerce, Interior, and DOJ. DHS generally agreed with our recommendations and provided comments that are discussed near the end of this letter. DHS's comments are contained in appendix V. FCC provided comments via e-mail and agreed with our recommendations, but raised concerns that related to the depth and scope of our analysis, such as stating that the report relies heavily on anecdotes and opinion. We made changes to clarify the scope of our work, but remain confident about our findings and conclusions. We discuss FCC's comments in detail near the end of this letter. The comments from Commerce and Interior are discussed near the end of this letter and contained in appendixes VI and VII, respectively. Interior commented that the report could have been improved by incorporating Interior or federal interoperability collaboration efforts in regards to emergency response capabilities. DOJ did not comment on the report. DHS, FCC, Commerce, and Interior also provided technical comments that we incorporated, where appropriate.

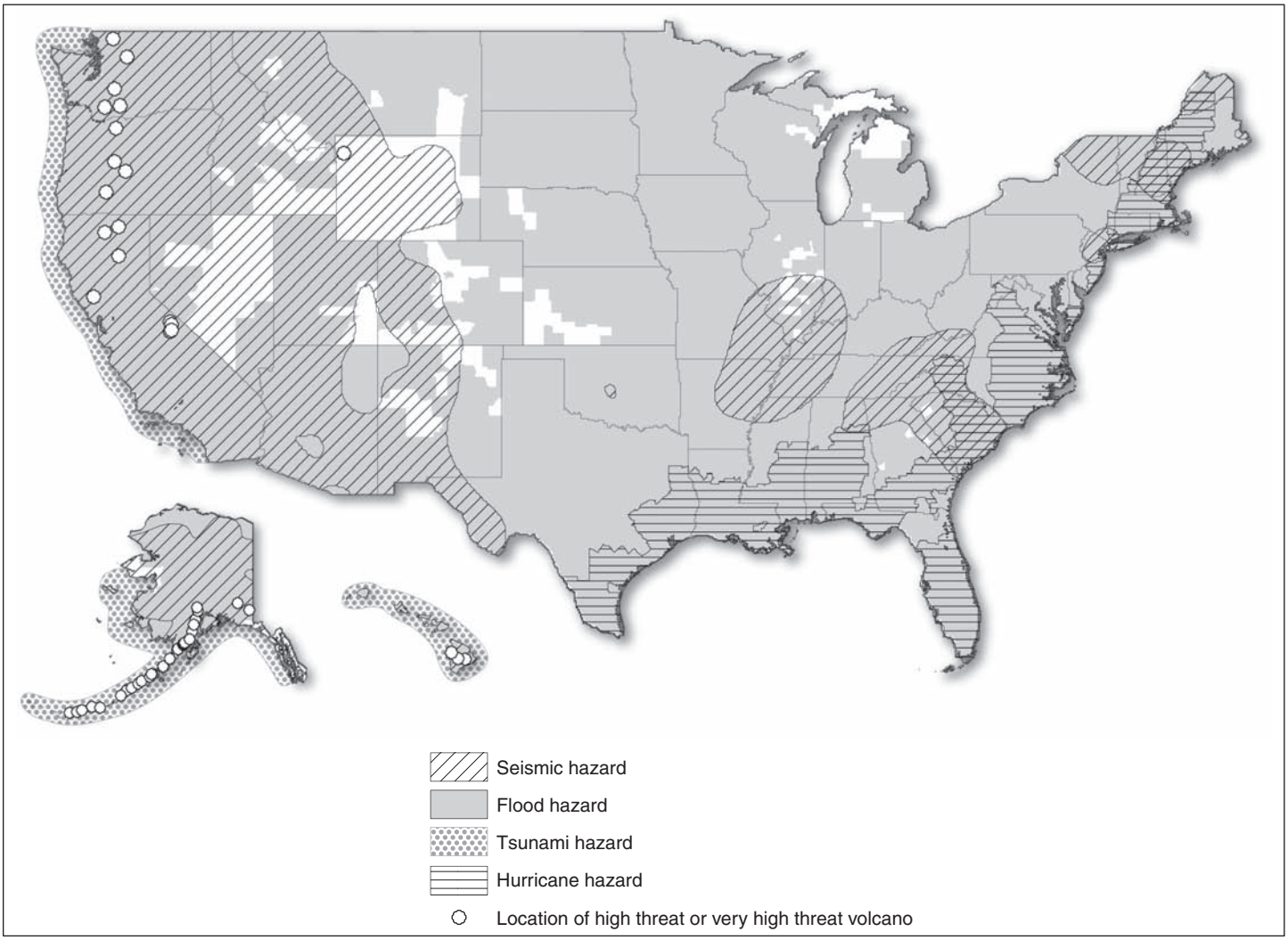
Background

Many regions of the country face hazards from natural and man-made disasters, some of which could prove catastrophic (see fig. 2). Unlike most typical disasters, catastrophic incidents can yield extraordinary levels of mass casualties, damage, or disruption, immediately overwhelming the response capacities of state and local resources, and requiring outside action and support from the federal government and other entities.[3] Some catastrophic disasters, such as large-scale hurricanes, may be detected or forecast well before they impact population centers, though their intensity and path can change significantly and quickly. Other catastrophic incidents, such as earthquakes and terrorist attacks, can occur with little or no notice. DHS has encouraged an all-hazards approach to disaster planning, to ensure that communities consider all threats faced, both natural and man-made, in the planning process. An all-hazards approach accounts for vulnerabilities, such as damage to infrastructure, that occur in various types of disasters in locations across the country. Some types of disasters, such as hurricanes, are more likely to occur in certain areas of the country, but many regions face hazards from one or multiple types of disaster. The goal of disaster preparedness and response is to prevent where possible, prepare for, or mitigate, and respond to disasters of any size or cause with effective actions at all levels of government that minimize the loss of life and property and set the stage for a quick recovery.[4]

[3]DHS's National Response Framework defines a catastrophic incident as any natural or man-made incident, including terrorism that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic incident could result in sustained nationwide impacts over a prolonged period of time; almost immediately exceeds resources normally available to state, tribal, local, and private-sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened. Department of Homeland Security, *National Response Framework*, 2008.

[4]GAO, *Homeland Security: DHS Improved Its Risk-Based Grant Programs' Allocation and Management Methods, but Measuring Programs' Impact on National Capabilities Remains a Challenge*, GAO-08-488T (Washington, D.C.: Mar. 11, 2008).

Figure 2: Examples of Natural Disaster Hazards in the United States



Sources: GAO analysis of Federal Emergency Management Agency (FEMA), National Oceanic and Atmospheric Administration (NOAA), and United States Geological Survey (USGS) data; Map Resources (map).

Note: Figure 2 depicts only those natural disasters included as part of our case study work and omits other disaster types, such as tornadoes. We derived hurricane hazards in the figure from hurricane strike data from 1980 through 2007. NOAA officials noted that the impact of hurricanes can be felt along the U.S. Gulf and Atlantic Coasts from Texas to Maine and extend inland for hundreds of miles.

First responders play a critical role in disaster preparedness and recovery, assisting in the response to emergency events, including catastrophic disasters. Typically, first responders include law enforcement, firefighters, emergency medical personnel, and others who are among the first on the scene of an emergency. However, since the terrorist attacks of September

11, 2001, the definition of first responder has grown to include other organizations, such as public health and hospital personnel, which may not be on the scene, but are essential in supporting effective response and recovery operations. Depending on the nature and location of a catastrophic event, responders on the scene may also include federal agencies directing all or a portion of the federal disaster response or assisting state and local first responders in their response efforts. For example, the Federal Bureau of Investigation (FBI) would participate in the response to a terrorist attack, based on its mission to protect and defend the United States against terrorist threats.

Communications systems serve as the backbone for first responders in gathering and sharing information, coordinating response, and requesting additional resources and assistance from neighboring jurisdictions and/or the federal government. Effective communications are vital to first responders' ability to respond and ensure the safety of both their personnel and the public. First responders cooperate to rescue victims, oftentimes relying on several different communications systems to do so. Voice, data, and video technology, if available, can be used to share information seamlessly between first responders, other various organizations, and different levels of government.

Recent catastrophic events have underscored the importance of emergency communications. For example, the 9/11 Commission concluded that the large number of deaths among firefighters during the collapse of the World Trade Center was partly attributable to a communications failure.[5] Following the September 11, 2001, terrorist attacks and Hurricane Katrina in 2005, Congress expanded a number of federal agencies' roles and responsibilities related to emergency communications. The Homeland Security Act of 2002 established DHS and required the agency, among other things, to build a comprehensive national incident management system comprising all levels of government and to consolidate existing federal government emergency response plans into a single, coordinated national response plan.[6] Hurricane Katrina highlighted additional communications challenges and demonstrated the need to improve emergency communications leadership at all levels of government in order to better respond to a catastrophic disaster.

[5]9-11 Commission, *The 9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: July 2004).

[6]Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

More recent legislation has directed DHS and FEMA to take on certain roles and actions related to emergency response and emergency communications. To address many of the challenges highlighted by the Hurricane Katrina response, the Post-Katrina Emergency Management Reform Act of October 2006 (Post-Katrina Act) was enacted, and established within DHS, the Office of Emergency Communications to help develop, implement, and coordinate interoperable and operable communications for the emergency response community at all levels of government.[7] The Office of Emergency Communications also oversees other DHS efforts, including elements of the SAFECOM program,[8] and the development of the National Emergency Communications Plan and other key documents intended to create an overarching strategy to address emergency communications shortfalls. The Post-Katrina Act also charged FEMA with the primary responsibility for coordinating and implementing key aspects of federal emergency preparedness and response, including grants management. As required by the act, FEMA is to lead and support the nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation. FEMA leads the integration of tactical federal emergency communications during disasters and often deploys personnel or equipment to the scene of a disaster to manage the federal response.

Other federal agencies also have a role in emergency communications and disaster response. For example, in September 2006, FCC established its Public Safety and Homeland Security Bureau, which is responsible for developing, recommending, and administering the agency's policies pertaining to public safety communications issues.[9] The bureau submits annual reports to the FCC Chairman and Commissioners and hosts quarterly summits on various topics relevant to the public safety community. In addition, the bureau has established a clearinghouse to

[7]The Post-Katrina Act was enacted as Title VI of the Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, 120 Stat. 1355 (2006). The provisions of the Post-Katrina Act became effective upon enactment, October 4, 2006, with the exception of certain organizational changes related to FEMA, most of which took effect on March 31, 2007.

[8]SAFECOM is a DHS communications program that provides research, development, testing and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, tribal, state, and federal emergency response agencies.

[9]These policies include 9-1-1 and E9-1-1; operability and interoperability of public safety communications; communications infrastructure protection, and disaster response; and network security and reliability.

collect, evaluate, and disseminate public safety information. FCC also manages the use of the radio-frequency spectrum by non-federal entities, such as commercial enterprises, state and local governments, and public safety organizations. Radio spectrum is a fixed, limited resource, which government and nongovernmental entities share for commercial and public safety communications.[10] In 1993, legislation authorized FCC to use competitive bidding—or auctions—to assign spectrum licenses to commercial users.[11] For the last several years, FCC has pursued a new Public/Private Partnership (the 700 MHz Public/Private Partnership) in a proceeding involving commercial and public safety spectrum in the 700 MHz Band, which was occupied by television broadcasters.[12] As part of the digital television transition, this spectrum was to be cleared and made available for public safety and commercial services in June 2009.[13] See figure 3.[14]

[10]Spectrum is divided into frequency bands, each having technical characteristics that affect electronic transmission in different ways. "Bandwidth" is related to the transmission capacity of a frequency band. If voice calls and low-rate data are involved, narrowband systems are adequate; but, to transmit video and images, broadband is needed.

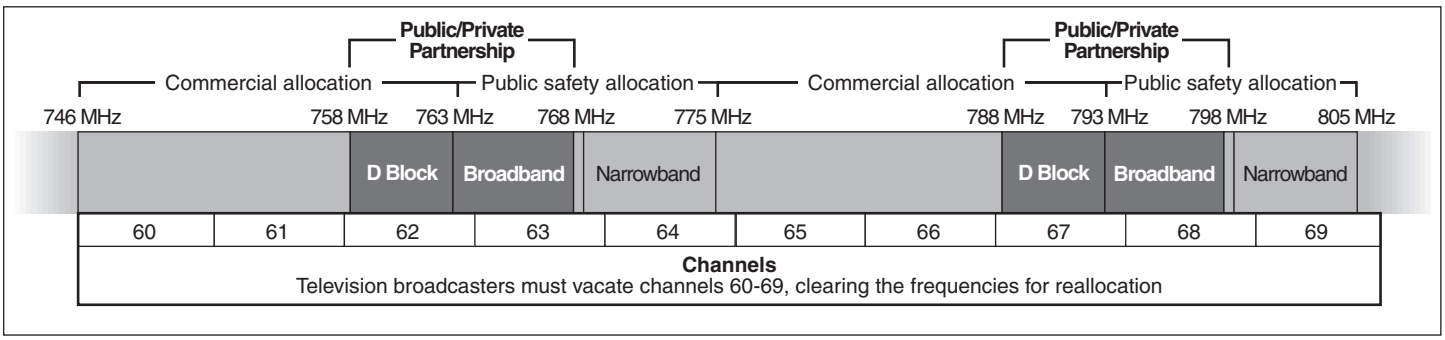
[11]Omnibus Reconciliation Act of 1993, Pub. L. No. 103-66, § 6002, 107 Stat. 312, 387-392 (1993), codified as amended at 47 U.S.C. § 309(j).

[12]In September 2008, FCC issued its Third Further Notice of Proposed Rulemaking in this proceeding. See, Service Rules for the 698-746, 747-762 and 777-792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, *Third Further Notice of Proposed Rulemaking*, 23 FCC Rcd 14301 (2008) (700 MHz).

[13]DTV Delay Act, Pub. L. No. 111-4, 123 Stat. 112. The act also extends the Commission's auction authority through September 2012.

[14]In the Public/Private Partnership, the winning bidder of the commercial license in the Upper 700 MHz D Block (758-763/788-793 MHz) ("D Block") is to partner with the nationwide licensee of the public safety broadband spectrum (763-768/793-798 MHz) ("Public Safety Broadband Licensee") to enable construction of an interoperable broadband network that would serve both commercial and public safety users.

Figure 3: Upper 700 MHz D Block and Public Safety Broadband Allocation



Source: NTIA and GAO.

Another agency with a role in emergency communications is the Department of Commerce's National Telecommunications and Information Administration (NTIA), which is responsible for managing spectrum used by the federal government.[15] Officials from NTIA and other agencies also serve on a number of interagency committees to coordinate their activities on a standing and disaster-activated basis. DHS's National Communications System (NCS) coordinates the emergency support function for communications, which involves, among other things, oversight of communications within the federal incident management and response structures. Interior has also been an active joint federal partner through the National Interagency Fire Center, which has provided search and rescue capabilities, as well as deploying, operating, and managing communications systems during recent disasters.

With a mission to ensure public safety against foreign and domestic threats, DOJ has also worked with other federal agencies, such as DHS and the Department of the Treasury, to improve disaster response. For example, in 2001, DOJ initiated an effort to provide secure, seamless, and interoperable wireless communications for federal agents and officers engaged in law enforcement, homeland defense, and disaster response.[16]

[15]NTIA is the President's principal adviser on telecommunications and information policy issues, and in this role frequently works with other Executive Branch agencies to develop and present the Administration's position on these issues.

[16]GAO, *Radio Communications: Congressional Action Needed to Ensure Agencies Collaborate to Develop a Joint Solution*, GAO-09-133 (Washington, D.C.: December 2008).

Multiple federal agencies have a role in disaster preparedness and response, and there are several best practices agencies can employ to help overcome the barriers to successful inter-agency collaboration. We have previously reported on collaboration best practices, which are useful in addressing issues that are national in scope and cross agency jurisdictions, such as emergency communications.[17] For the purposes of our report, we focus on the three best practices described in table 1. Prior GAO work has also shown that monitoring and evaluating agency actions and progress can help key decision-makers obtain feedback for improving both policy and operational effectiveness.[18]

Table 1: Best Practices in Collaboration

Collaboration practice	Description
Define and articulate a common outcome	Collaboration requires agency staff working across agency lines to define and articulate the common federal outcome or purpose they are seeking to achieve that is consistent with their respective agency goals and mission.
Establish mutually reinforcing or joint strategies	To achieve a common outcome, collaborating agencies need to establish strategies that work in concert with those of their partners or are joint in nature. Such strategies help in aligning the partner agencies' activities, core processes, and resources to accomplish the common outcome.
Identify and address needs by leveraging resources	Collaborating agencies bring different levels of resources to the effort. Collaborating agencies can look for opportunities to address resource needs by leveraging each other's resources, thus obtaining additional benefits that would not be available if they were working separately.

Source: GAO.

To improve emergency preparedness, states, regions, and local jurisdictions have also invested billions to build dedicated networks and acquire technology, lease or subscribe to private carrier services for primary or backup systems, and to maintain and test existing communications systems. Similarly, private stakeholders, such as telecommunications companies and equipment manufacturers, have invested heavily to develop innovative technological solutions and expand or strengthen their networks for

[17]GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: October 2005); and GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996).

[18]GAO/GGD-96-118 and GAO-06-15.

emergency responders and commercial use. Private stakeholders develop proprietary technology and networks that first responder agencies may buy, lease, or subscribe to by paying service charges (see app. III for an overview of some of the various technologies that first responders use).

Continuity of Communications, Capacity, and Interoperability Are Primary Areas Where Emergency Communications Remain Vulnerable

Continuity of communications, capacity, and interoperability are the primary areas of vulnerability in emergency communications that persist in communities across the country. We identified these vulnerabilities in interviews with state and local first responders in each of our six case studies and others, as well as a review of emergency communications literature, which include our prior work. DHS and FCC have identified similar vulnerabilities in recent work, including continuity of communications and interoperability.[19] First responders also noted that identified communications vulnerabilities extend beyond the communities in our case study locations and that other disaster scenarios pose similar hazards.

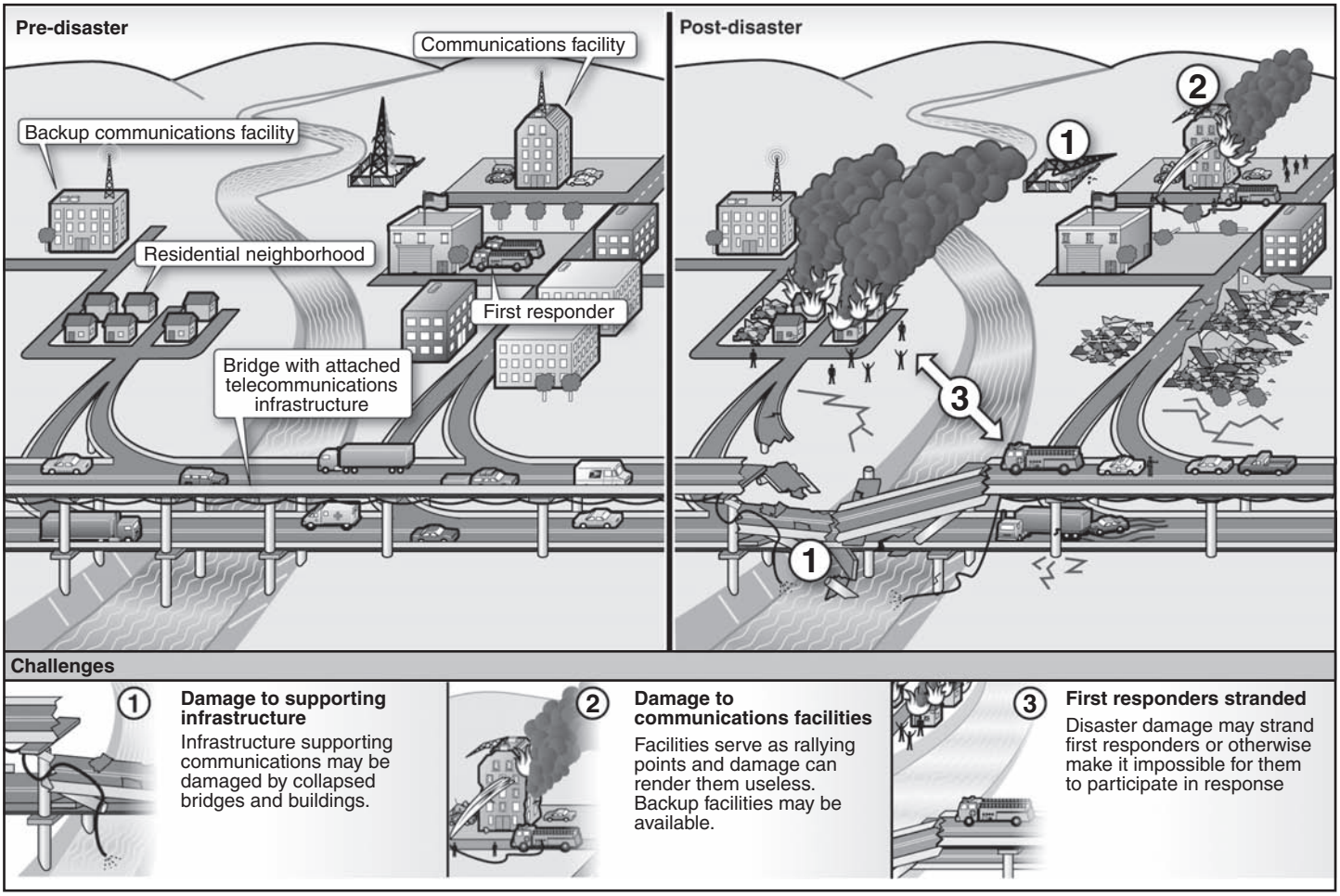
Catastrophic Disasters Threaten Continuity of Communications

Destructive forces, such as high winds and ground shaking, during catastrophic disasters can disrupt first responders' continuity of communications—the ability to maintain communications during and following a disaster—in a number of ways. Using the scenario of a major earthquake in a city, figure 4 depicts how damage to supporting infrastructure and communications facilities, as well as stranding first responders, may threaten continuity of communications.[20]

[19]FCC, however, would not necessarily characterize "continuity of communications" as a vulnerability; rather, FCC views this as a goal for emergency communications systems.

[20]While based on our case studies, we do not intend figure 4 or other figures depicting disaster scenarios and their effects on emergency communications to represent effects at any particular location that we visited. An actual catastrophic disaster could have much larger and more complicated impacts. The figure is meant to provide examples of just some of the ways in which communications may be disrupted.

Figure 4: Vulnerabilities Involving Continuity of Communications in an Earthquake Scenario



Source: GAO.

Damage to Supporting Infrastructure. Communications systems used by first responders, such as landline phone systems and certain radio systems, cannot function without phone cables, radio towers, and other supporting infrastructure. For example, Hurricane Katrina's high winds and flooding destroyed emergency communications infrastructure in Louisiana and Mississippi, disrupting continuity of communications in several states and inhibiting the response. Potential, future catastrophic disasters pose similar hazards, such as a lahar—a volcanic mudflow—in

Mount Rainier National Park in Washington state.[21] National Park Service officials stationed in the park said that the park's telephone system relies on a privately-owned phone cable, which is old and exposed in many locations (see fig. 5). According to park officials, keeping the cable operational is a constant challenge even under normal circumstances. In the event of a lahar at Mount Rainier, fast-moving mud and debris could destroy the cable and disrupt the park's phone system (see app. II for more information on the hazards associated with our six case studies).

[21]A lahar is a volcanic mudflow that originates from the slopes of a volcano. These flows contain rock and other debris that exert high impact force against objects in their path, such as buildings and trees. Sizes vary, but lahars can travel over 50 miles from a volcano. Triggers for lahars include volcanic eruptions and massive landslides, such as the one that occurred at Mount St. Helens in the state of Washington in 1980.

Figure 5: Exposed, Hanging Cable at Mount Rainier National Park

Source: GAO.

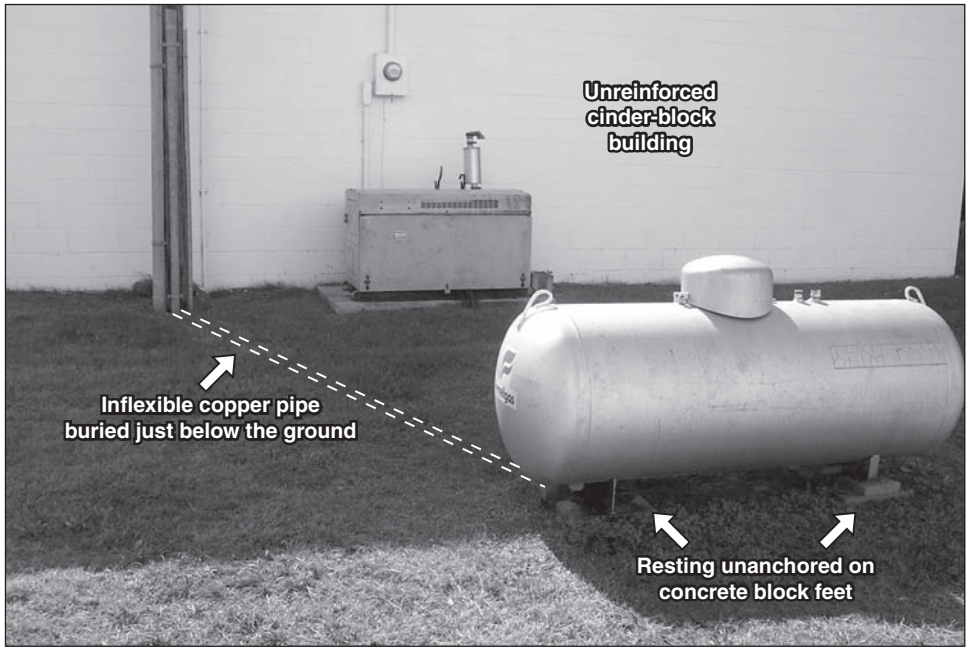
Damage to Communications Facilities. Emergency operations centers[22] and other facilities serve as command posts from which first responders coordinate and launch a response. Yet a disaster may damage or destroy these facilities, rendering them useless. First responders in Jackson, Tennessee, described intense tornadoes hitting and damaging two emergency operations centers in 2003, which then inhibited the response. Responders in Jackson and Memphis, Tennessee, also said that some of their facilities were vulnerable to future earthquakes generated in the New Madrid seismic zone.[23]

[22]An emergency operations center is the physical location where multiagency coordination occurs. The core functions of such a center include coordination, communications, resource allocation and tracking, and information collection, analysis, and dissemination for disaster response.

[23]The New Madrid seismic zone is a collection of fault lines that runs through several states, including Arkansas, Missouri, Illinois, Kentucky, and Tennessee. The zone has produced several major earthquakes since 1800. Geologists expect similar earthquakes in the future.

Local facilities were not constructed to withstand seismic shaking, and some are located on thick sediment, which can amplify seismic shaking. Even if a facility experiences little direct damage, the disaster may down power lines to the facility, which some communications systems need to function. Officials at the National Public Safety Telecommunications Council described maintaining power as the most basic vulnerability facing emergency communications after a disaster. Officials at the Central United States Earthquake Consortium[24] noted that facilities in Tennessee and neighboring states have backup power generators. However, some fuel tanks powering the generators are not properly secured and may otherwise be vulnerable to seismic shaking (see fig. 6).

Figure 6: Vulnerable Fuel Tank in the New Madrid Seismic Zone



Sources: The Central United States Earthquake Consortium (photograph); and GAO.

[24]Established in 1983, the consortium's primary mission is to reduce deaths, injuries, property damage, and economic losses from earthquakes in the central United States. The organization's primary objective is to support multi-state response and recovery planning, resource acquisition; public education and awareness; promotion; mitigation, and research associated with earthquake preparedness in the central United States. Members include Alabama, Arkansas, Illinois, Indiana, Kentucky, Mississippi, Missouri, and Tennessee.

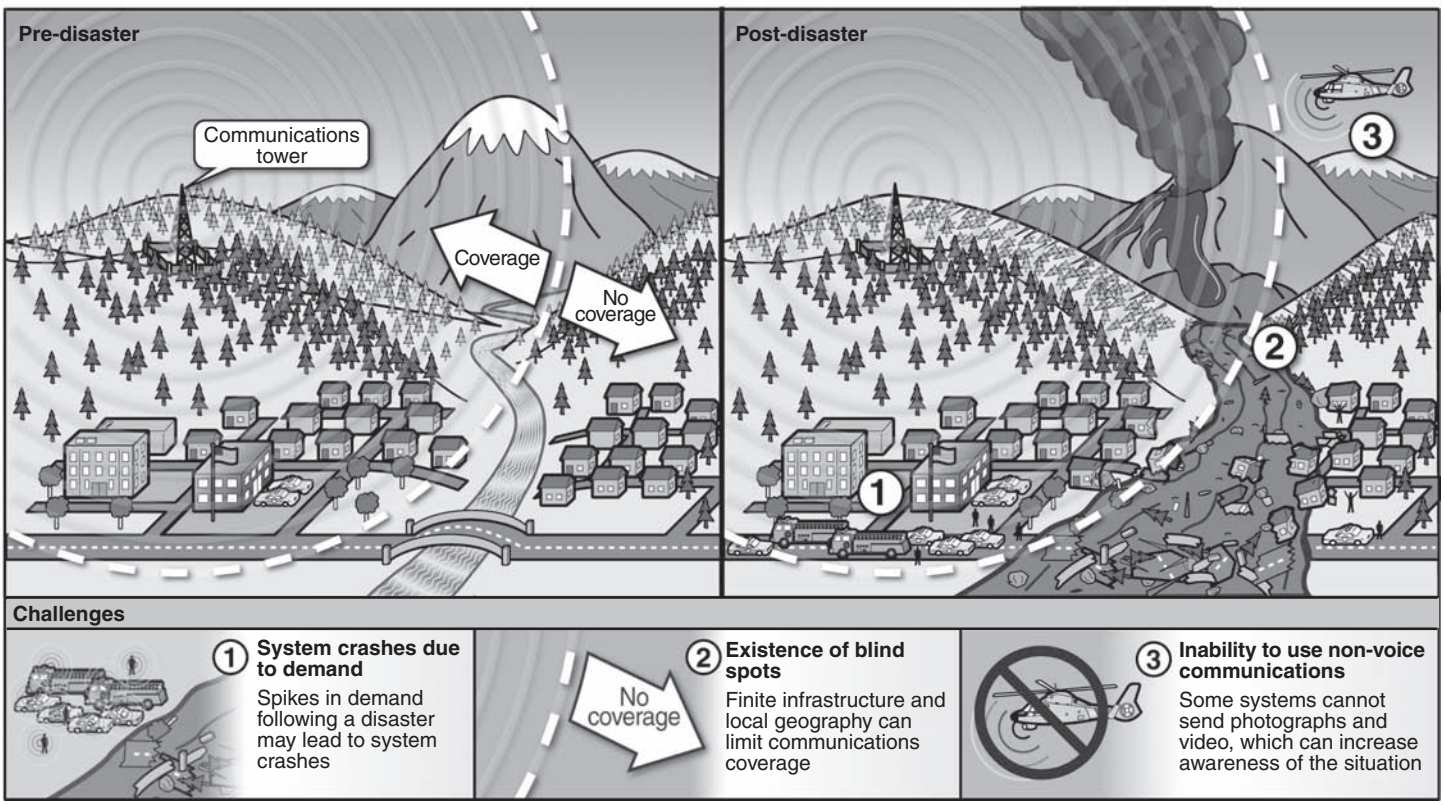
To help maintain continuity of communications, some jurisdictions have designed facilities to withstand damages expected from future disasters. For example, Miami-Dade County officials described mitigating potential hurricane wind damage at a county communications facility by adding a sloped roof. First responders in Memphis, Tennessee reported that some newer facilities had been built to supposedly resist seismic shaking. Tennessee and California first responders identified backup locations that they would move to if their facilities were damaged, but this move would take time before they would regain full communications capabilities.

Stranded First Responders. Disasters may strand first responders or otherwise make it impossible for them to participate in a response. Following Hurricane Katrina, many state and local first responders were incapacitated and flooding blocked access. This inhibited response by preventing the establishment of a command structure for the response, reducing communications and awareness of the situation following Hurricane Katrina's landfall. Memphis first responders expressed concerns that a future, major earthquake in the New Madrid seismic zone will damage bridges and strand some first responders across the Mississippi River in Arkansas. With the Mississippi river bisecting the region, bridges are some of the most important and seismically vulnerable piece of the transportation network. A majority of the bridges were designed with little or no seismic consideration. Law enforcement and fire department officials in Tennessee, Florida, and Washington state conveyed concerns about the ability of their staff to report after a major disaster. Damage to first responders' property, as well as personal injury to themselves or family, can also prevent participation in response. To address such difficulties and maintain continuity of communications, Miami-Dade County has taken steps to enable responders' families to shelter in local facilities and to help repair first responder property damage.

Limited System Capacity Hinders First Responders' Communications

A number of capacity issues can hamper emergency communications systems used in disaster response. For our work, we use the term "capacity" to refer to a communication system's ability to handle demand, provide coverage, and send different types of information (i.e., voice and data). Using the scenario of a lahar hitting a small town, figure 7 depicts how capacity may be threatened by system crashes due to demand, the existence of blind spots, and an inability to use non-voice communications.

Figure 7: Vulnerabilities Involving Capacity Limitations in a Lahar—Volcanic Mudflow—Scenario



Source: GAO.

System Crashes due to Demand. Some communications systems used by first responders may lack the capacity to prevent system crashes due to spikes in demand, which can follow disasters. Telecommunications company officials reported that their systems are not designed to handle everyone in a region calling simultaneously. Past disasters, such as the terrorist attacks in 2001 and Hurricane Katrina in 2005, created excessive demand, which caused communications system to crash. System outages can also place additional

demands on remaining systems. More recently, officials in the California Governor's Office of Emergency Services reported that over 5 million calls followed a moderate earthquake and disrupted communications for a short time. FCC has reported that first responders enjoy communications capabilities that are more robust than those provided by the private sector; yet, communications also rely on the functioning of the 85 percent of the nation's critical communications infrastructure that the private sector controls. Boston Fire Department officials told us that they anticipate reduced communications capabilities following a disaster due to system crashes. Jurisdictions are working to increase capacity on public and private sector communications systems and related infrastructure. For example, some jurisdictions are building new fiber optic networks. In addition, some telecommunications companies offer jurisdictions services for additional system capacity in a disaster, such as "cell on wheels" and "cell phone on light trucks," to restore communications.[25]

Existence of Blind Spots. Communications system "blind spots"—that is, areas that lie outside the range of local communications systems—exist for a number of reasons. Some communications systems have finite infrastructure, such as radio systems with a limited number of towers and effective transmission range. In addition, local geography can create blind spots as elevation changes or high-rise buildings interfere with radio signals. We observed instances of system blind spots in our case studies. According to Hawaii first responders, mountainous terrain has created blind spots for some communities near the water, which could inhibit emergency communications and response during a tsunami.[26] Law enforcement officials in one of our other case study locations also reported that some local tunnels are blind spots for certain emergency communications systems in the area. Jurisdictions are addressing blind spots

[25]These assets are mobile, self-contained cell sites to boost coverage for first responders. They are designed for short-term response and can process thousands of calls per hour.

[26]Underwater earthquakes typically generate tsunamis—landslides, volcanic activity, and meteor strikes are less common sources. Tsunami generating earthquakes usually occur in subduction zones, such as those found in the Pacific Ocean off the U.S. western and Alaskan coasts. Subduction zones are formed where one of the earth's outer shell of tectonic plates plunges underneath another. A tsunami's size depends on the earthquake's size, its depth below the ocean floor, the type and amount of seafloor movement and the energy released among other factors. Some tsunami waves can travel up to 600 miles-per-hour, hitting nearby coasts within minutes and other distant shorelines hours later. We have previously reported on communications challenges related to tsunamis. See GAO, *U.S. Tsunami Preparedness: Federal and State Partners Collaborate to Help Communities Reduce Potential Impacts, but Significant Challenges Remain*, GAO-06-519 (Washington, D.C.: June 5, 2006).

by investing in mobile communications vehicles. In the event of an existing blind spot, or damage from a disaster creating new ones, these vehicles can plug gaps in emergency communications coverage by establishing a mobile communications network at or near the scene of an incident. Vehicles are equipped with cellular and satellite phone and fax capabilities, an on-board computer network, printers and satellite, internet access, video teleconferencing, recording, and broadcast/satellite television (see fig. 8). However, such assets are not a cure all for blind spots and may not be able to support all organizations responding to a disaster.

Figure 8: Jurisdictions' Emergency Response Vehicles

Jackson Police Department communications vehicle

Interior of the Jackson Police communications vehicle, showing a work desk with two computer monitors and wireless Internet

Boston Fire Department communications vehicle

Pierce County communications vehicle

Source: GAO.

Inability to Send Non-Voice Communications. Some current systems are not designed to send non-voice communications, such as photographs and video. First responders in several of our case study areas described additional capabilities that developing non-voice communications would provide. For example, photographs and video can quickly convey an

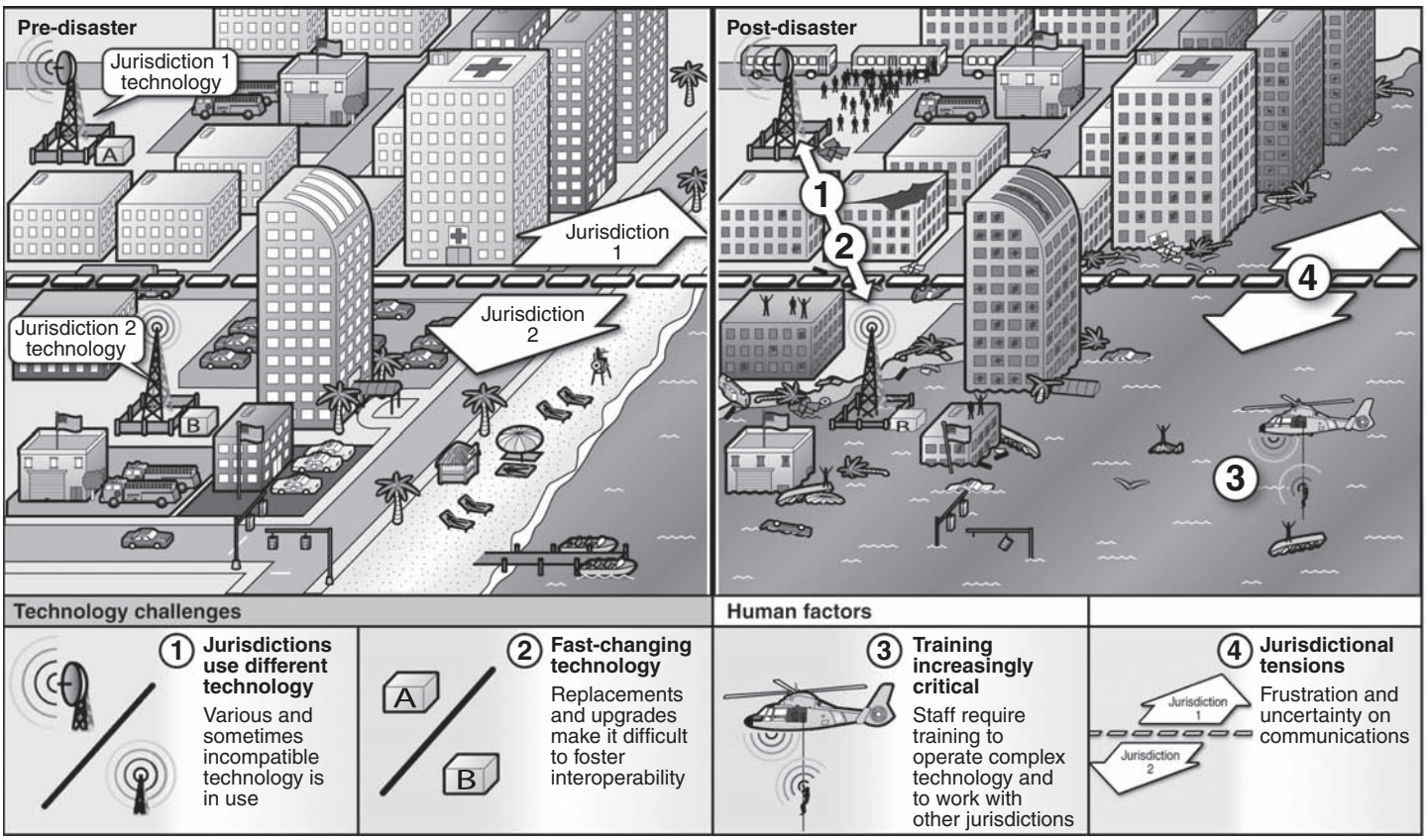
emergency situation, saving time in response. Related capabilities, such as geospatial mapping, can accurately identify the location of first responders relative to a disaster. Hawaii first responders described an instance battling brush fires when air reconnaissance had to roughly convey its location using voice descriptions compared with a paper map. Some jurisdictions we interviewed are expanding, or planning to expand, their systems' capacity to transmit photographs and videos. For example, first responders in Sacramento, California, have planned to install a digital radio system in their emergency operations center, which would enable both voice and data transmissions.

Interoperability Vulnerabilities Persist

We have previously reported on vulnerabilities involving interoperability, which is the ability of first responders to communicate with whomever they need to (including personnel from a variety of agencies and jurisdictions), when they need to, and when they are authorized to do so. Facilitating interoperability has been a concern for many years, and we have cited a variety of obstacles to effective interoperable communications among first responders.[27] While we have reported on progress in improving interoperability among first responders, our case study work shows that technological and human factors continue to impair interoperability. Using the scenario of a hurricane hitting a coastal city, figure 9 depicts how interoperability may be threatened by jurisdictions using different technologies, fast-changing technologies, the critical nature of training, and jurisdictional tensions.

[27]GAO, *First Responders: Much Work Remains to Improve Communications Interoperability*, GAO-07-301 (Washington, D.C.: Apr. 2, 2007).

Figure 9: Vulnerabilities Involving Interoperability in a Hurricane Scenario



Source: GAO.

Jurisdictions Use Different and Fast-Changing Technology. First responders continue to use various, and at times, incompatible communications technology, making it difficult to communicate with neighboring jurisdictions or other first responders to carry out response. For example, some fire departments have hesitated to use digital radio systems due to safety concerns, which could create incompatibility with other responders' equipment, such as law enforcement (see app. III for

more information on communications systems used by first responders).[28] According to first responders in Tennessee, Massachusetts, and Washington state, 800 MHz radio systems perform poorly in buildings. Difficult radio communications in high-rise buildings contributed to firefighter deaths during the September 11, 2001, terrorist attacks in New York City as some firefighters did not receive the transmission to evacuate the World Trade Center. In another example, Hawaii's geographic isolation has contributed to island jurisdictions independently designing their communications systems, resulting in disparate systems statewide. This can prove problematic for interoperability, particularly if a major disaster required responder assistance from neighboring islands.

Given the fast-changing nature of communications technology, upgrade needs and replacement cycles compound interoperability vulnerabilities. Officials at the National Public Safety Telecommunications Council reported that keeping up with technology is difficult for jurisdictions due to funding constraints. Yet some jurisdictions must upgrade when manufacturers eliminate technical support for older systems. Other legacy systems still in use are aging or obsolete. For example, some communications systems currently used by California's first responders have reached or exceeded their life expectancy, while other components need replacement. Not all jurisdictions, however, maintain the same upgrade schedule. For example, first responders in Pierce County, Washington, described coordinated efforts by them and other jurisdictions to help ensure that different technological upgrades and other system changes increase rather than reduce existing interoperability.

To account for different and sometimes incompatible communications systems, some jurisdictions have used technologies to facilitate interoperability by "patching" together different systems into a common network. For example, first responders in Florida, Massachusetts, and Washington state described using equipment to create a local area network that can patch in different communications systems. This patched network can create local interoperability among different jurisdictions'

[28]Spectrum allocations for state and local public safety are fragmented into many distinct slices of the radio spectrum. Bands of interest to public safety include VHF (very high frequency), and UHF (ultra high frequency). Radio systems used by law enforcement and other first responders operating in the 806-824 MHz and 851-869 MHz portion of the UHF bands are often referred to as "800 MHz" systems. The 800 MHz band is also home to commercial wireless carriers and private radio systems. In July 2004, the FCC adopted a comprehensive plan to reconfigure the 800 MHz band to separate public safety systems in the band from commercial wireless systems using cellular architecture.

communications systems. However, first responders noted instances where patching technology failed to establish interoperability.[29] Also, some patching equipment cannot provide blanket interoperability for an entire city or county and thus may be insufficient to meet communications needs in a catastrophic incident.

Human Factors. Several jurisdictions emphasized that training was increasingly critical to operate complicated equipment and coordinate with multiple jurisdictions to improve interoperability. The Massachusetts Executive Office of Public Safety and Security reported that achieving interoperability not only requires equipment, but staff must be regularly trained to work effectively with a number of jurisdictions. According to the 9-11 Commission Report,[30] the New York City Police and Fire Departments were not prepared to comprehensively coordinate with one another on the day of the September 11, 2001, terrorist attacks. This led to communications breakdowns where responding agencies lacked knowledge of what other agencies were doing. For example, firefighters did not receive information from police helicopters regarding damage to the World Trade Center. There were also jurisdictional tensions as some reports indicated that firefighters refused to evacuate when asked by police officers, contributing to deaths. We observed jurisdictional tension in several of our case studies, which could inhibit cooperation and achieving interoperability. First responders in Florida, Massachusetts, and Washington state noted frustration with neighboring jurisdictions and uncertainty over how jurisdictions would communicate in the event of a disaster. Working well with others and reducing tensions has taken on increasing importance as more jurisdictions, such as public works, are regarded as first responders and participate in emergency communications. Memphis first responders said that achieving interoperability requires not only compatible technology, but also jurisdictions building relationships among personnel.

[29]FCC officials noted limitations with patched networks. For example, handsets programmed to operate on frequencies not supported by base stations in the same area will still not be able to communicate with each other unless there is a compatible base station with which the handset can communicate.

[30]*The 9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.*

A Wide Range of Federal Assistance Aimed at Helping First Responders Mitigate Emergency Communications Vulnerabilities

Federal agencies such as DHS and FCC have a wide range of assistance intended to help first responders mitigate emergency communications vulnerabilities. Available assistance includes federal agency guidance, grants, and technical support. We have identified several examples of key federal assistance used by first responders.[31]

New Strategic Guidance among Significant Federal Efforts to Enhance Emergency Communications

DHS and other federal agencies have recently developed strategic guidance and pursued significant efforts to enhance emergency communications. Efforts such as the National Emergency Communications Plan, the Emergency Communications Preparedness Center, and various stakeholder and advisory groups reflect an emphasis on developing a more strategic approach to federal government efforts to mitigate emergency communications vulnerabilities. Other recent efforts underway include FCC's new approach to establishing a 700 MHz Public/Private Partnership.

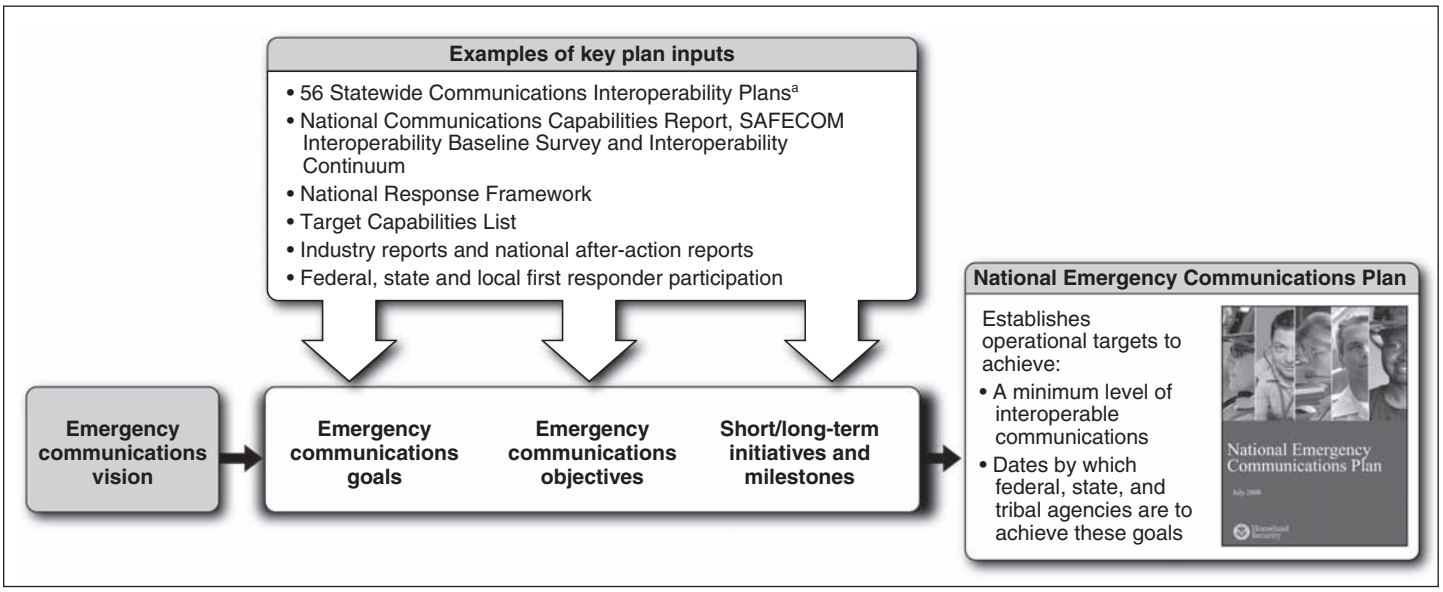
National Emergency Communications Plan. DHS's Office of Emergency Communications released the National Emergency Communications Plan in July 2008, providing a framework for emergency communications users across all levels of government.[32] The plan is the first strategic document focused exclusively on improving emergency communications nationwide, and outlines an overarching strategy to address emergency communications shortfalls for federal, state, and local first responders. The plan includes strategic emergency communications goals and objectives, and recommends numerous initiatives and milestones to guide emergency response providers and government officials in making

[31]Our examples do not constitute a complete list, or evaluation of the effectiveness of, this federal assistance currently available to first responders. We have previously reported on a number of issues/challenges in past disaster preparedness efforts. See GAO-09-133; GAO-07-301; GAO, *Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-740 (Washington, D.C.: July 2004).

[32]Department of Homeland Security, *National Emergency Communications Plan* (Washington, D.C.: July 2008).

measurable improvements to emergency communications (see fig. 10). Congress required this plan—developed with federal, state, local, and private sector stakeholder involvement and multiple policy and planning documents—to be subject to periodic review and updates. An important foundation for the plan, the National Communications Capabilities Report—also released in July 2008—provides a framework for evaluating the emergency communications capabilities of federal, state, and local agencies and organizations, which, according to the report, vary.[33] Both of these reports build on the groundwork set by the 2004 DHS SAFECOM Interoperability Continuum, which recognizes the importance of a formal governance structure to ensure the success of interoperability planning, including improving the policies and procedures of major projects by enhancing stakeholder coordination and establishing guidelines and principles.

Figure 10: National Emergency Communications Plan Framework



Source: GAO analysis of DHS information.

[a]The 56 Statewide Communications Interoperability Plans include the District of Columbia and 5 territories.

[33]Department of Homeland Security, *National Communications Capabilities Report* (Washington, D.C.: July 2008).

Emergency Communications Preparedness Center. The Post-Katrina Act requires federal agencies including DHS, FCC, DOJ, and the Department of Commerce to establish and jointly operate the Emergency Communications Preparedness Center.[34] Under the act, the center is intended to serve as the focal point and clearinghouse for intergovernmental emergency communications information sharing, and is required to submit to Congress an annual strategic assessment on federal coordination to advance emergency communications. The Emergency Communications Preparedness Center is to provide a governance and decision-making structure for strategic interagency coordination of emergency communications at the federal level. The center will not be officially established until a MOU has been finalized and approved by the signatory agencies.[35] DHS's Office of Emergency Communications chairs the Emergency Communications Preparedness Center working group. The working group drafted a charter, which defines the mission and roles of its members. Once approved, the charter will serve as the MOU governing the Emergency Communications Preparedness Center. As of June 2009, the agencies were working on completing the MOU.

700 MHz Public/Private Partnership. The FCC is pursuing a 700 MHz Public/Private Partnership to promote a nationwide interoperable broadband network for public safety that would increase the bandwidth capacity available for first responders in both day-to-day operations and during an emergency response. This has been a key FCC effort with regards to emergency communications and is a significant departure from prior FCC public safety spectrum allocations, which assigned spectrum licenses on a jurisdiction-by-jurisdiction basis. However, after the first attempt to auction the nationwide D Block license did not result in a winning bidder, FCC issued two further notices of proposed rulemakings, and a final order has not been adopted.[36] According to statements in FCC's Third Further Notice, a public/private partnership remains the best option to achieve nationwide build-out of an interoperable broadband network for public safety, given the current absence of federal appropriations for

[34]The Emergency Communications Preparedness Center membership has since been broadened to include other federal agencies beyond those specified in the Post-Katrina Act.

[35]Interior is also a charter member of the Emergency Communications Preparedness Center, and the agency has participated in the Charter writing and review process.

[36]The D Block refers to the portion of commercially allocated spectrum that is adjacent to the public safety broadband spectrum. The March 2008 auction received only a single bid that did not meet the reserve price of $1.33 billion and thus did not become a winning bid.

this purpose and the limited funding available to the public-safety sector. In April 2009, FCC officials reported that they were exploring ideas and options for future use of the spectrum. While the ultimate outcome of the 700 MHz Public/Private Partnership is currently unknown, the proceeding has involved significant FCC action over the course of several years (see table 2).

Table 2: 700 MHz Public/Private Partnership Proceeding

700 MHz Public/Private Partnership: Major Actions	
August 1997	Congress allocated 24 megahertz of spectrum in the Upper 700 MHz Band for public safety services.[a]
December 2006	FCC proposed a centralized and national approach to maximize public safety access to interoperable, broadband spectrum in the 700 MHz band, and to foster and promote the development and deployment of advanced applications (e.g., data and video), technologies, and systems.[b]
July 2007	FCC created a nationwide license in the D Block and required the winning commercial bidder to work with the Public Safety Broadband Licensee in a Public/Private Partnership—governed by FCC rules and a network sharing agreement—to construct and operate a nationwide network shared by commercial and public safety users.[c]
November 2007	The Public Safety Spectrum Trust was granted the license for the Public Safety Broadband Licensee.[d]
March 2008	FCC's Auction 73 failed to attract a winning commercial bidder for the D Block of spectrum.[e]
September 2008	FCC proposed a modified set of rules and a revised auction plan in the Third Further Notice, which includes a proposal to use the bidding process to determine whether the D Block spectrum would be licensed on a nationwide or regional basis.[f]
November 2008	The Third Further Notice public comment period closed, and FCC was continuing to review comments as of June 2009.

Source: GAO analysis of FCC information.

[a]See Balanced Budget Act of 1997, Pub. L. No. 105-33, 111 Stat. 251 § 3004 (1997) (adding § 337 of the Communications Act); Reallocation of Television Channels 60-69, the 745-806 MHz Band, Report and Order, 12 FCC Rcd 22953 (1998), recon. 13 FCC Rcd 21578 (1998).

[b]See Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, Ninth Notice of Proposed Rulemaking, 21 FCC Rcd 14837 (2006) (700 MHz Public Safety Ninth Notice).

[c]700 MHz Second Report and Order, 22 FCC Rcd 15289 (2007).

[d]Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, Order, 22 FCC Rcd 20453 (2007).

[e]See Auction 73, 700 MHz Band, at http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=73.

[f]700 MHz Third Further Notice of Proposed Rulemaking, 23 FCC Rcd 14301 (2008). See, also 700 MHz Second Further Notice of Proposed Rulemaking, 23 FCC Rcd 8047 (2008).

Stakeholder Groups and Advisory Committees. DHS and FCC have established stakeholder groups and advisory committees to help leverage existing knowledge and provide strategic recommendations to improve emergency communications. The purpose of these groups is to contribute expertise, recommendations, and lessons learned from recent disasters to help improve emergency communications. For example, the FCC's Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks studied the effect of Hurricane Katrina on all sectors of the telecommunications and media industries, including public safety communications.[37] The panel then reviewed the sufficiency and effectiveness of the recovery effort and made recommendations to FCC regarding ways to improve disaster preparedness, network reliability, and communications. More detailed information on these emergency communications related groups and committees—including missions and activities—can be found in appendix IV.

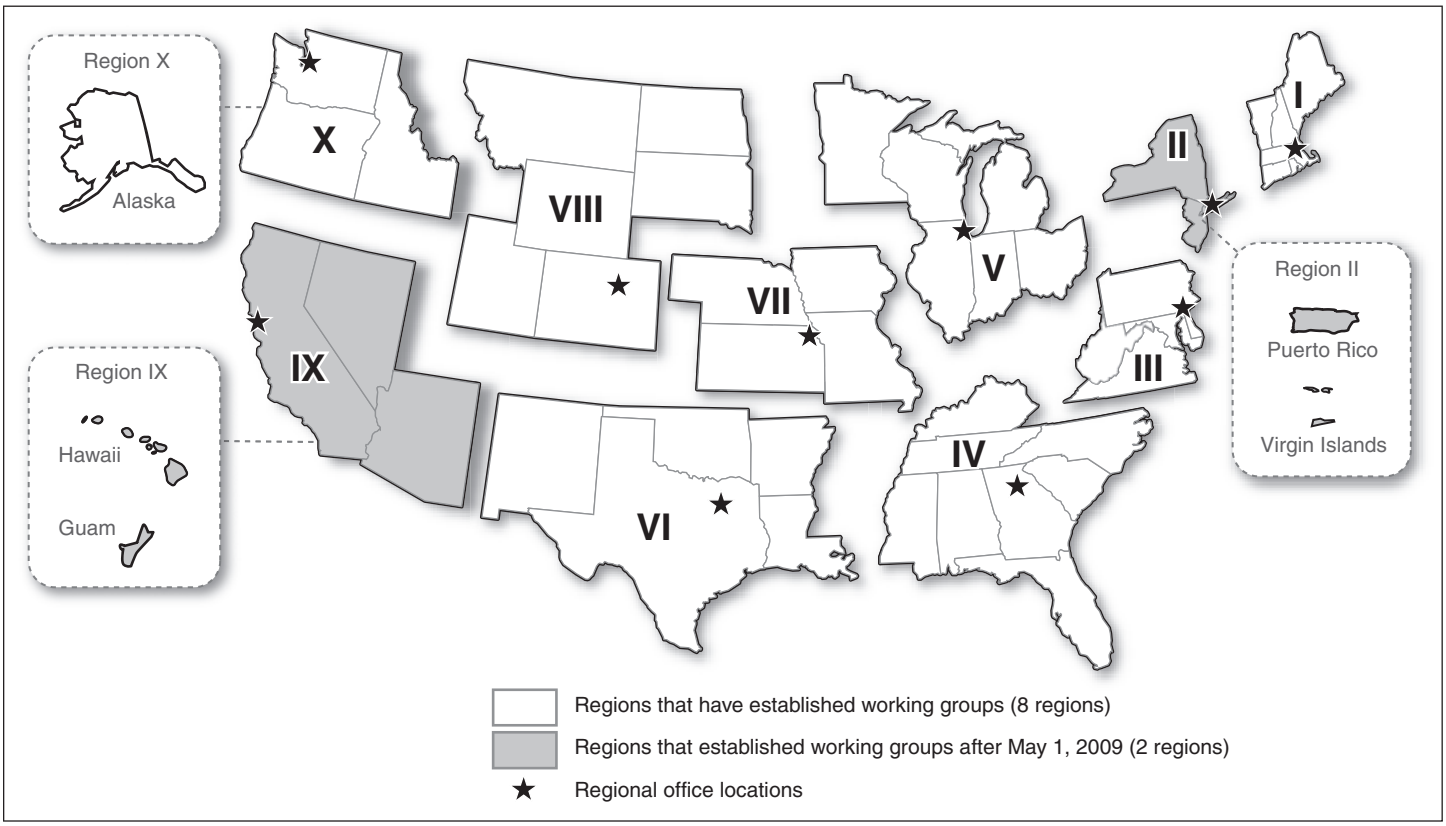
Regional Emergency Communications Coordination Working Groups. As required by the Post-Katrina Act, and in an effort to develop a new regional governance structure, FEMA has recently established 10 Regional Emergency Communications Coordination Working Groups (see fig. 11), intended to work closely with federal, state and local officials to improve emergency communications.[38] Specifically, the working groups are to assess local emergency communications systems' ability to meet the goals of the National Emergency Communications Plan; facilitate disaster preparedness by promoting multi-jurisdictional and multi-agency emergency communications networks; and ensure activities are coordinated with regional emergency communications stakeholders. FEMA has proposed that the working groups be the single federal emergency communications coordination point for disaster response and interaction with state and local governments. Many of the established working groups are in early stages of development. For example, the Region X working group—covering Mount Rainier in Washington state—has held one stakeholder meeting. As of June 2009, all 10 of the FEMA

[37]The Federal Advisory Committee Act, 5 U.S.C. App. 2, governed the operations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks with guiding principles of openness in government; diversity in membership and advice; and public accountability.

[38]The Post-Katrina Act directs these working groups to be established in each of the 10 FEMA regional offices and to include DHS, FCC, and other federal agencies with responsibility for coordinating interoperable emergency communications or providing emergency support services. 6 U.S.C. § 575.

Regions had established working groups. In addition, FEMA has hired 1 national and 10 regional positions to coordinate these working groups.

Figure 11: Status of Regional Emergency Communications Coordination Working Groups



Source: FEMA (data); MapArt (map).

A Variety of Federal Funding Available

Federal agencies have several grants available for states, territories, and local and tribal governments that are used for emergency communications. In 2008, interoperable emergency communications represented the largest investment category of DHS grants, including more than a dozen grant programs such as the Urban Areas Security Initiative,[39] the State

[39]The Urban Areas Security Initiative is intended to enhance regional preparedness for prevention, protection, response, and recovery in 62 major metropolitan areas determined to be "highest risk."

Homeland Security Initiative,[40] the Interoperable Emergency Communications Grant Program,[41] and the Emergency Operations Center Grant Program.[42] FEMA, which is responsible for allocating and administering DHS grants, awarded over $3.85 billion in federal funding to improve interoperable emergency communications to state and local agencies from 2004 to 2007. FEMA manages the majority of federal grants for disaster preparedness and response; however, other federal agencies have contributed to this effort. The total amount of federal funds directed to emergency communications interoperability in the last 8 years is difficult to determine because after the September 11, 2001, terrorist attacks, multiple federal agencies offered funding to state and local governments in preparation for natural and man-made disasters. Interoperability was among several grant criteria for broad preparedness funds that could be used for a number of things, including interoperable emergency communications.

Historically, DOJ has also contributed to emergency communications efforts. Many first responders in our case study locations reported that they received funding to improve emergency communications from DOJ grant programs. For example, Boston, Honolulu, and Miami participated in DOJ's 25 Cities Project,[43] which funded initiatives to address communication networks between key state and local authorities in major metropolitan areas that were determined to be at a higher risk for terrorist attack. Boston, Memphis, and Sacramento also received funding from

[40]The State Homeland Security Initiative provides funds to states and territories to implement the goals and objectives of state homeland security strategies and initiatives included in the State Preparedness Report.

[41]The Interoperable Emergency Communications Grant Program provides governance, planning, training and exercise, and equipment funding to state, territories, and local and tribal governments to carry out initiatives to improve interoperable emergency communications. We provide more details on this program later in our report.

[42]The Emergency Operations Center Grant Program supports Emergency Operations Centers with a focus on addressing identified deficiencies and needs.

[43]The 25 Cities Project refers to the High-Risk Metropolitan Area Interoperability Assistance Project, a DOJ Wireless Management Office grant program that identified the top 25 metropolitan areas that were considered likely targets for terrorist attack and provided communication solutions to federal and local authorities such as fire, police, and emergency medical services. Projects differed from city to city.

DOJ's Interoperable Communications Technology Program,[44] which funds local and regional voice and data interoperability projects. Between 2003 and 2006, the Community Oriented Policing Program invested over $250 million in 65 agencies to improve jurisdictions ability to talk across disciplines such as fire and police departments using radio communications networks. In 2007, DOJ awarded $5.7 million to the Sacramento Police Department to support technology projects facilitating voice and data information sharing.

More recent federal funding has largely come from DHS and been focused on addressing specific gaps and identified needs, such as interoperable emergency communications. In 2007, all 56 states and territories received a portion of the approximately $1 billion, one-time Public Safety Interoperable Communications Grant Program funding to purchase hardware and update technology for interoperable communications systems. These funds were provided to assist public safety agencies in the planning and coordination associated with the acquisition of, deployment of, or the training for the use of interoperable communication equipment, software, or systems. The Public Safety Interoperable Communications Grant Program is an NTIA program. NTIA and DHS signed a joint collaboration agreement to have FEMA administer the grant program. This funding assists public safety agencies in improving communications through investments identified by each state or territory's Statewide Communications Interoperability Plan (SCIP), which FEMA required prior to release of grant funds.

The Post-Katrina Act required DHS to ensure consistency between grant guidelines and the goals and recommendations of the National Emergency Communications Plan. Requiring states to develop SCIPs was one step in an overall effort to align DHS-administered funding with the National Emergency Communications Plan. In developing the SCIPs, states involved local agencies and stakeholders to help identify communication and interoperability gaps to better address vulnerabilities (see fig. 12). The plans were developed using a methodology, which identified and developed working groups or governance councils to assure state-level accountability. For example, to ensure that local, regional, tribal, and state needs would be addressed and coordinated, California combined efforts of its existing

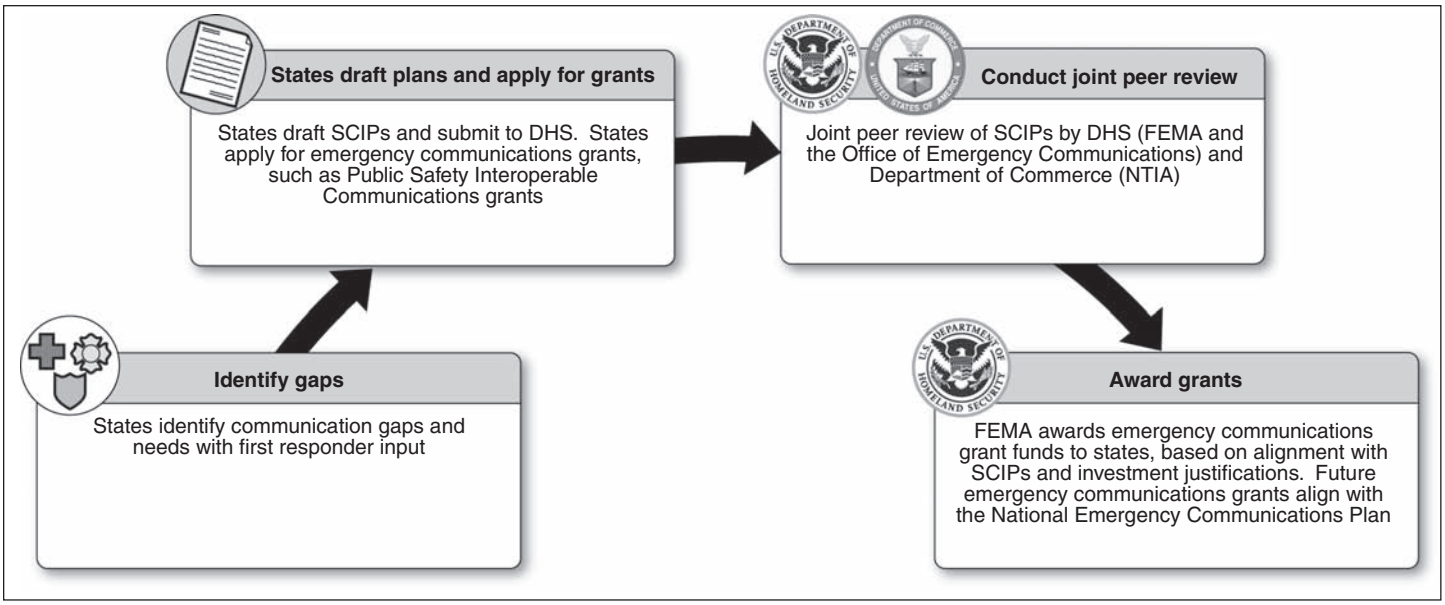
[44]The Community Oriented Policing Interoperable Communications Technology Program funded projects that used equipment and technologies to increase interoperability among the law enforcement, fire service, and emergency medical service communities from fiscal years 2003 through 2006.

Statewide Interoperability Executive Committee with other strategic planning groups. The Office of Emergency Communications, FEMA, and NTIA jointly oversaw a peer review of the SCIPs and the investment justifications, using panels to review both documents, in order to ensure that Public Safety Interoperable Communications investment justifications addressed gaps that had been identified in the SCIPs. The Office of Emergency Communications used the recommendations from the peer review to approve the SCIPs in February 2008, and FEMA and NTIA used the information from the peer review to approve the investment justifications. All states where our case studies were located developed plans and received funding through the 2007 Public Safety Interoperable Communications grant[45] ranging from $8.1 million for Hawaii to $94 million for California. California is using some of these funds to pursue 16 statewide communications initiatives, including enhancing and implementing interoperability in the Sacramento area.

Beginning in 2008, FEMA and the Office of Emergency Communications worked together to develop the Interoperable Emergency Communications Grant Program. Whereas the Public Safety Interoperable Communications Grant was a one-time investment, this new grant program is ongoing and is intended to help enable state, territorial, and local governments to implement their SCIPs. The program funds initiatives in governance, planning, equipment, training, and exercises that are consistent with the strategic initiatives and milestones outlined in the National Emergency Communications Plan. The Interoperable Emergency Communications Grant Program awarded $48.6 million in both fiscal years 2008 and 2009.

[45]While we did not evaluate the effectiveness or quality of the Public Safety Interoperable Communications Grant Program as a part of our work, a recent Department of Commerce Office of Inspector General report identified an issue regarding Public Safety Interoperable Communications grant effectiveness. The report found that most grantees have made little progress in implementing their projects, and much remains to be done for the grantees to finish their projects by the September 30, 2010, deadline. See *Public Safety Interoperable Communications Grant Program: Grantees Appear Unlikely to Finish Projects Within Short Funding Time Frame*, Final Audit Report No. DEN-19003 (Washington, D.C.: March 2009).

Figure 12: Public Safety Interoperable Communications Grants and Efforts to Align Targeted Investments for First Responders with the SCIP



Source: GAO analysis of DHS information.

Technical Support and Federal Assets Are Intended to Help Mitigate Emergency Communications Vulnerabilities

Several federal agencies with a role in disaster response offer technical support and initiatives in advance of an incident, or some can provide federal assets at the scene of a disaster to help mitigate emergency communications vulnerabilities. Federal agencies such as DHS and DOJ have developed technical support offerings intended to assist first responders in advanced planning and emergency preparedness. Similarly, in response to a real-time incident, DHS and FEMA can establish a physical presence at the disaster site, deploying personnel and assets to assist first responders. Technical support and planning provide assistance to address individual state and local jurisdictions' emergency communications needs. The following programs and efforts are examples of technical assistance and training available to assist first responders in improving continuity of communications, capacity, or interoperability, among other vulnerabilities.

- *Interoperable Communications Technical Assistance Program*. DHS's Interoperable Communications Technical Assistance Program provides support to first responders for planning and technical issues that need to be considered when first responders develop interoperable communications. The program supplies a site management team and

support to each area requesting assistance, providing technical assistance and analysis tailored to meet site-specific requirements. All of our case study scenario states have received technical assistance and services through this program. For example, Hawaii received assistance on 17 work requests, including communications unit leader training, a tabletop exercise,[46] and engineering support. Many states also used this technical assistance to aid in the development of their SCIPs. As previously discussed, DHS and FEMA also provided feedback to assist states in completing these plans, as well as input to assure alignment with the National Emergency Communications Plan.

- *Catastrophic Disaster Response Planning Initiative*. In 2006, FEMA began a Catastrophic Disaster Response Planning Initiative combining planning and exercises to produce functional plans for areas at risk of a catastrophic disaster. In this ongoing effort, communications is one of several functional areas FEMA is addressing with state and local first responders. This involves planning for disaster scenarios—including a catastrophic earthquake in the New Madrid seismic zone and a hurricane in Florida—two of our case study locations. In the earthquake-planning scenario, for example, FEMA officials are focused on a bottom-up approach (i.e., beginning at the local level across all disciplines, then rolling up to the state level to identify gaps and craft the regional plan to mitigate those gaps) and completed 14 local workshops and 18 state-level workshops in 2008, which included approximately 3,800 stakeholders at all levels of government.
- *Government Emergency Telecommunications Service and Wireless Priority Service*. NCS's Government Emergency Telecommunications Service provides subscribers with access cards for priority service over wireline telephone networks in an emergency.[47] The FCC and NCS's Wireless Priority Service offers a similar service for cellular networks, and both of these services can be useful in mitigating capacity vulnerabilities when demand overwhelms communications systems immediately following an incident. State and local first responders in many of our case

[46]A tabletop exercise is a discussion-based exercise that focuses on existing plans, policies, mutual aid agreements, and procedures used among multiple agencies. Typically, a tabletop exercise involves representatives from the entire range of agencies and jurisdictions that would take action in all-hazards or terrorist response incidents.

[47]The Government Emergency Telecommunications Service uses a calling card that provides access authorization and priority treatment to first responders in the public switched telephone network through a unique dialing plan and personal identification number, and is designed to maximize all available telephone resources should outages occur during a disaster or other emergency.

study locations participated in the Government Emergency Telecommunications Service program. NCS also manages the Telecommunications Service Priority Program, which provides national security and emergency preparedness users priority authorization of telecommunications services.

- *Integrated Wireless Network*. In 2001, DHS, DOJ, and the Department of the Treasury began a collaborative effort to develop the Integrated Wireless Network and provide secure, seamless, and interoperable wireless communications for federal agents and officers engaged in law enforcement, homeland defense, and disaster response. Initially conceived as a joint radio communications solution to improve communication among federal, state, and local law enforcement agencies, the Seattle/Blaine area in Washington state began a pilot network in 2004. While the pilot continues to provide service to multiple agencies, the departments have determined that this specific system design cannot be implemented on a nationwide scale. Consequently, the formal governance structure that was initially established among the three departments has been disbanded, and the contract for developing a new design is not currently being used jointly by the departments for this purpose.
- *Project 25*. The Association of Public Safety Communications Officials' Project 25 is a long-standing effort to select common system standards for digital public safety radio communications.[48] These standards are intended to allow radios to be interoperable regardless of manufacturer. We have previously reported that implementation of systems based on incomplete Project 25 standards has been problematic.[49] With no process in place to confirm that equipment advertised as compliant actually met the standards, Congress called for the creation of the Project 25 Compliance Assessment Program.[50] This voluntary program establishes a process for equipment suppliers to submit their equipment to certain testing labs to receive a certification of Project 25 compliance.[51]

[48]Project 25 was initiated in 1989.

[49]See GAO-07-301. Project 25 radios were marketed to and purchased by federal, state, and local agencies without any formal compliance testing to validate vendors' compliance with the standards.

[50]See S. Rep. No. 109-88, at 45 (2005); H.R. Rep. No. 109-241, at 81 (2005).

[51]The initial Compliance Assessment Program process began in December 2008, and after a 6-month grace period, equipment covered by the program that is purchased with federal grant dollars will be accompanied by declarations of compliance and test reports.

In response to a disaster, federal assets are also available on the ground to help mitigate one or more emergency communications vulnerabilities, including continuity of communications, capacity, and interoperability. Some emergency response personnel and equipment may be deployed to the scene, such as DHS and FEMA officials, while other federal agencies may have personnel at the scene based on the nature and/or location of the incident. For example, at Mount Rainier National Park in Washington state, National Park Service personnel physically located on site would be directly involved in any response effort taking place within the park. Some federal agencies have assets available that can be deployed during or immediately following an incident and can help mitigate continuity of communications vulnerabilities. For example, FEMA maintains 6 deployable Mobile Emergency Response Support detachments across the country. These detachments provide personnel, vehicles, and technology on the scene and can help other federal agencies, state, or local first responders establish communications. Mobile Emergency Response Support detachments can be activated at the request of state authorities to provide communications on the scene when existing state and local communications infrastructure has been damaged or destroyed. For example, some of the vehicles in the detachment have the communications equipment necessary to facilitate full voice, data, and video multi-agency interoperability and can operate as a stand-alone communications center. The Maynard, Massachusetts, detachment was deployed 41 times in 2007, 34 times in 2008. Based on its proximity to one of our case study locations, the Bothell, Washington, detachment could be an effective tool for restoring communications after a catastrophic disaster at Mount Rainier, as equipment and personnel could arrive on scene within 12 hours after an incident (see fig. 13).

Figure 13: FEMA Mobile Emergency Response Support Vehicle

Source: GAO.

Limited Collaboration and Monitoring Jeopardize Significant Federal Efforts and Impede Progress

Limited collaboration and monitoring impedes the progress of some significant efforts being undertaken by federal agencies to strategically enhance emergency communications. Our past work has shown, and the National Emergency Communications Plan articulates, that collaboration and monitoring are important elements to advancing emergency communications.[52] We found that federal agencies have demonstrated limited application of collaboration best practices, as well as lack mechanisms for fully monitoring efforts.

[52]The mission of FCC's Public Safety and Homeland Security Bureau is to collaborate with others, including other federal agencies. Specifically, the mission is "To collaborate with the public safety community, industry, and other government entities to license, facilitate, restore and recover communications services used by the citizens of the United States, including first responders, before, during and after emergencies by disseminating critical information to the public and by implementing the Commission's policy initiatives."

Collaboration Key to Advancing Emergency Communications

Defining a common goal and mutually reinforcing strategies are collaboration best practices that can help federal agencies deal with issues that are national in scope and cross agency jurisdictions.[53] In particular, establishing a governance structure that includes defined leadership, roles, and responsibilities can be an effective step for establishing goals and aligning strategies so that they are mutually reinforcing.[54] Addressing goals by leveraging resources is another collaboration best practice that can be employed across agencies to maximize resources. The National Emergency Communications Plan acknowledges the importance of collaboration, including at the federal level, for enhancing emergency communications. Among the plan's seven objectives is that federal emergency communications programs and initiatives be collaborative and aligned to achieve national goals. Additionally, the plan speaks to the importance of federal programs and initiatives related to emergency communications being coordinated so as to minimize duplication, maximize federal investments, and ensure interoperability.

Strong collaboration is especially important since DHS has limited authority to compel other federal agencies to participate or align their emergency communications activities despite DHS's leadership role in compiling and overseeing the National Emergency Communications Plan. DHS officials noted that the agency cannot unilaterally achieve the strategic goals, initiatives, and milestones of the National Emergency Communications Plan and will rely on the voluntary commitment of federal, state, local, and tribal government officials and the private sector.[55] DHS's tools to encourage the participation of stakeholders include the technical assistance that DHS's Office of Emergency Communications provides to state, regional, local, and tribal government officials and the development of grant policies that align with the National Emergency Communications Plan. The agency has fewer instruments to encourage federal agencies' participation. For example, the National Communications Capabilities Report notes that federal agencies are not

[53]GAO/GGD-96-118 and GAO, *Electronic Government: Potential Exists for Enhancing Collaboration on Four Initiatives*, GAO-04-6 (Washington, D.C.: October 2003).

[54]GAO-09-133. See also, GAO-06-15, GAO/GGD-96-118, and GAO-04-6.

[55]Similarly in 2004, GAO reported that SAFECOM's authority and ability to oversee and coordinate federal and state efforts for increased interoperability was limited by its dependence upon other agencies for funding and their willingness to cooperate. GAO, *Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration*, GAO-04-494 (Washington, D.C.: April 2004).

eligible to receive grants, and therefore, grant guidance is an ineffective means for encouraging and coordinating federal participation.

Establishing Common Goals and Mutually Reinforcing Strategies Can Enhance Some Significant Emergency Communications Efforts

In our past and current work, we found that federal agencies have demonstrated limited application of certain collaboration best practices with respect to some significant federal efforts.[56] Limited collaboration has contributed to the failure of past federal emergency communications efforts and puts ongoing efforts at risk.

Integrated Wireless Network. In December 2008, we reported that federal efforts to provide a joint agency solution for federal emergency communications through the Integrated Wireless Network had not been successful, because federal agencies did not effectively identify a common goal and design mutually reinforcing strategies.[57] We found that success depended on a means to overcome differences in agency missions and cultures and a joint strategy to align activities and resources to achieve a joint solution. More specifically, DHS, DOJ, and the Department of the Treasury did not establish an effective governance structure. In abandoning collaboration as a joint solution, DHS, DOJ, and the Department of the Treasury risk duplication of effort and inefficient use of resources as they continue to invest significant resources on independent solutions. Further, the efforts being pursued by these three agencies will not ensure that vulnerabilities involving interoperability are addressed. We have previously reported that interoperability with federal first responders remains an important element in achieving nationwide interoperability, and until a federal coordinating entity makes a concerted effort to promote federal interoperability with other governmental entities, overall progress in improving communications interoperability will remain limited.[58]

Emergency Communications Preparedness Center. Delays in establishing the Emergency Communications Preparedness Center undermine implementation of the National Emergency Communications Plan's wide array of strategic goals, initiatives, and milestones scheduled to occur concurrently—most of which within the first year from the plan's July 2008

[56]Collaboration can be broadly defined as any joint activity that is intended to produce more public value than could be produced when the organizations act alone.

[57]GAO-09-133.

[58]GAO-07-301.

issuance—and depend on cooperation from multiple agencies to achieve. The National Emergency Communications Plan describes that milestones detail the timelines and outcomes of each of the 29 initiatives to serve as the "key checkpoints" to monitor the plan's implementation. To that end, the plan includes 11 January 2009 milestones, 2 April 2009 milestones, and 41 July 2009 milestones. These milestones scheduled to occur within the first year of the plan's issuance comprise more than half of the plan's total 91 milestones. As previously discussed, the Post-Katrina Act envisions the center will serve as a focal point for federal interagency coordination, and the National Emergency Communications Plan articulates that the center will help ensure that the strategic goals, initiatives, and milestones of the plan are agreed upon and that federal agencies work collaboratively to pursue mutually reinforcing strategies. The Office of Emergency Communications within DHS chairs the Emergency Communications Preparedness Center working group, which has drafted a MOU currently under review. As we have previously reported, an important element of establishing effective collaborative relationships is to reach formal agreements with each partner organization on a clear purpose, expected outputs, and realistic performance measures, which the center's MOU could supply.[59] In September 2008, DHS officials reported to Congress that the center's MOU was going to be completed by December 2008.[60] To date, the MOU has not yet been finalized. DHS officials reported to us that they are taking steps to establish the Emergency Communications Preparedness Center, but noted that the complexity of obtaining agreement from multiple agencies was a challenge. In the absence of the Emergency Communications Preparedness Center's finalized MOU, according to DHS officials, staff-level working groups are working to help implement the plan. With the final nature of the center as yet undetermined, however, FEMA officials expressed that many federal agencies and components are still functioning in an independent manner, which can be confusing to state and local first responders. Moreover, these officials' understanding of the center was that it would largely serve as a Web site clearinghouse for information. Other DHS officials reported that the center would serve a range of functions for emergency communications.

[59] GAO-04-6.

[60] *Interoperability in the Next Administration*: *Assessing the Derailed 700 MHz D Block Public Safety Spectrum Auction*: Hearing Before the House Subcommittee on Emergency Communications, Preparedness, and Response, 110th Cong. (Sept. 16, 2008).

DHS Efforts and FCC's 700 MHz Public/Private Partnership. Collaboration between DHS and FCC on the 700 MHz D Block spectrum has been limited. Spectrum is a valuable resource for public safety wireless communications, and the 700 MHz spectrum that is becoming available as the result of the digital television transition represents a significant increase for public safety purposes. Limited collaboration jeopardizes the viability and usefulness of this spectrum for public safety and its relation to other federal efforts. By employing collaboration best practices, DHS and FCC could enhance what is ultimately done with the 700 MHz broadband spectrum and help accomplish the goals of the National Emergency Communications Plan.[61]

DHS and FCC officials do not have a common vision for the 700 MHz spectrum and have expressed varying views on the relationship between the 700 MHz Public/Private Partnership—FCC's current proposal for how the 700 MHz should be allocated and assigned—and the National Emergency Communications Plan.[62] According to DHS officials, FCC's proceeding to establish the 700 MHz Public/Private Partnership directly supports the goals of the National Emergency Communications Plan and FCC officials said that they believed their effort is compatible with the National Emergency Communications Plan. However, FCC officials also reported that they believed the National Emergency Communications Plan applied to only existing emergency communications systems and, therefore, was not directly relevant to allocating and assigning the spectrum, which they believed to be the main purpose of the 700 MHz Public/Private Partnership proceeding.[63] FCC officials described the plan and the 700 MHz Public/Private Partnership proceeding as two separate

[61]Congressional members have expressed interest in the relationship between DHS, the Emergency Communications Preparedness Center, the National Emergency Communications, and the 700 MHz Public/Private partnership proceeding.

[62]FCC has taken steps to leverage DHS expertise on other efforts such as the 700 MHz narrowband requirement for mandatory interoperability through the use of Project 25 standards, as well as designated interoperability channels.

[63]FCC officials strongly assert that FCC must take into account input from all stakeholders, not just the views of DHS.

and parallel efforts.[64] These officials reported that, accordingly, it was reasonable that the proceeding's notices and other documents did not reflect or reference the National Emergency Communications Plan.

DHS's Office of Emergency Communications Director reported that it was too early for the office to have any significant role in developing the 700 MHz Public/Private Partnership, because the auction had not been completed.[65] DHS did not submit formal comments in this proceeding.[66] FCC officials stated that the lack of formal comments and critique from DHS suggested that the agency had no objections to the proposed rulemaking, and that it reflected the separate nature between the proceeding and DHS's efforts. FCC officials could not recollect nor provide us with a record of substantive conversations with DHS officials on this proceeding. However, the Director of DHS's Command, Control and Interoperability Division reported conveying to FCC officials several challenges regarding its 700 MHz Public/Private Partnership network before FCC's most recently issued document describing the proposed network, the Third Further Notice, was released. We recognize that FCC considers input from stakeholders, but also acknowledge DHS's important role in federal efforts regarding emergency communications. We compared the challenges this official expressed to any treatment in the Third Further Notice. Our analysis shows that on these issues that DHS and FCC do not share a common view in support of a 700 MHz Public/Private Partnership to build a nationwide, interoperable broadband

[64]According to DHS officials, while the National Emergency Communications Plan does not reflect the FCC's final policies for the 700 MHz Public/Private partnership, one of the key objectives of the plan (Objective 4: Standards and Emerging Communications Technologies) identifies a number of initiatives to ensure that emerging technologies, such as the wireless broadband technologies in the 700 MHz spectrum, are fully integrated with current emergency communications capabilities and work to improve interoperability on a nationwide basis.

[65]At a congressional hearing, members expressed interest in DHS officials providing their opinion on how FCC's 700 MHz proceeding should be structured.

[66]NTIA, acting on behalf of interested federal agencies, did submit formal comments on this proceeding. As previously discussed, NTIA has a role in managing spectrum used by federal agencies. Accordingly, discussions on the 700 MHz Public/Private Partnership that deal specifically with spectrum issues and access for federal agencies would include NTIA.

network.[67] (See table 3.) We recognize that FCC's efforts are ongoing and that no final decision relative to the future of the 700 MHz public safety broadband spectrum has yet been made.

Table 3: DHS Command, Control and Interoperability Division -identified Challenges to FCC's 700 MHz Public/Private Partnership

Challenges identified by DHS Command, Control and Interoperability Division	FCC Third Further Notice
Pursuing a business model that requires subscriptions would be problematic for jurisdictions that lack funds.	FCC proposed a standard charge of $7.50 per month per user (meaning per public safety officer/individual) for gateway-based access to the shared network(s).
Local jurisdictions hesitate to spend more money to buy additional equipment, since they have already spent billions in newer communications equipment and infrastructure that must be maintained for mission-critical voice communications.	FCC recognized that "multi-band radios could be developed, although at some cost…that are capable of operating on both the shared wireless broadband network and other public safety frequency bands." Additionally, FCC "tentatively concluded to require the Upper 700 MHz D Block licensee to offer gateway-based access . . ." but proposed that "public safety users themselves bear the costs of the bridges and gateways, including installation and maintenance costs…"
Distributing any associated equipment in a disaster situation would pose a logistical challenge, if not be impossible.	FCC did not address this issue of how associated equipment needed in a disaster area would be dispersed, but sought comment on whether "it should require use or availability of multi-band radios that could be available to public safety first responders that may need to come into these areas in times of emergency…"
Training and maintaining skills in using the network would be challenging, as first responders would need to use and exercise with this network often to maintain their familiarity with it.	FCC did not address or seek comment on if or how the proposed system would be made available for training and exercises.[a]

Source: GAO analysis of DHS and FCC information.

[67]The Congressional Research Service (CRS) has also highlighted the separate paths that DHS and FCC are pursuing in developing a national capabilities approach. Specifically, CRS stated that according to testimony "neither agency has undertaken to incorporate each other's goals in their specific planning." U. S. Congressional Research Service, *Public-Private Partnership for a Public Safety Network: Governance and Policy* (RL 34054, Oct. 16, 2008) by Linda K. Moore.

[a]According to FCC officials, mandating training requirements for state and local entities is outside FCC's jurisdiction. However, FCC officials also reported that it was possible for FCC to set conditions for the licensees operating the 700 MHz Public/Private Partnership to address such issues through its rulemaking process.

According to FCC officials, it would be the responsibility of the Public Safety Broadband Licensee to ensure that the network aligns with and furthers the goals of the National Emergency Communications Plan when it negotiates the details of the network sharing agreement with the winning commercial bidder. According to FCC officials, the Public Safety Broadband Licensee must ultimately meet the provisions outlined in the final rules adopted by FCC. It is unclear, however, how the Public Safety Broadband Licensee would do so or if it would have the authority to require such an alignment between the proposed network and DHS efforts. FCC did not suggest or specify in the Third Further Notice that the Public Safety Broadband Licensee consider the strategic goals and milestones of the National Emergency Communications Plan. Also, FCC did not in the Third Further Notice solicit comments on the relationship between the 700 MHz Public/Private Partnership and other DHS efforts. For example, FCC outlined no role for Regional Emergency Communications Coordination Working Groups, despite potential overlap with the 700 MHz Public/Private Partnership.[68] Specifically, the Public Safety Broadband Licensee is responsible for representing public safety interest in negotiating the network sharing agreement. In comparison, as legislatively defined and described within the National Emergency Communications Plan, the working groups are comprised of public safety officials who will assess emergency communications capabilities within their respective regions, facilitate disaster preparedness through the promotion of multijurisdictional and multiagency emergency communications networks, and serve as a primary link in coordinating multistate operable and interoperable emergency response initiatives and plans among federal, state, local, and tribal agencies. These working groups could provide a valuable means for representing public safety interests regionally and coordinating the use of a nationwide, interoperable, public safety broadband network envisioned by FCC.

Based on further analysis of the Third Further Notice and interviews with FCC and DHS officials, we found potential opportunities to align the proposed 700 MHz Public/Private Partnership network with the National

[68]At a congressional hearing, members expressed interest in the relationship between FCC's 700 MHz Public/Private Partnership and the Regional Emergency Communications Coordination Working Groups.

Emergency Communications Plan and other DHS efforts to reinforce one another.[69]

- Given the National Emergency Communications Plan's focus on Urban Area Security Initiative regions and the national planning scenarios and their continued use by DHS and FEMA, FCC could align the performance benchmarks to prioritize Urban Areas Security Initiative regions or reference in their definition of "emergency," DHS and FEMA's national planning scenarios.[70] FCC's 700 MHz Public/Private Partnership currently has no relationship to these efforts.
- FCC's Third Further Notice does not propose a specific role for state government in coordinating their public safety providers' participation in the 700 MHz Public/Private Partnership or the network, but state governments have played a key role in emergency communications by coordinating and completing SCIPs, which have been reviewed by DHS and were required to be eligible for federal funding.[71] FCC could consider ways to involve state government or integrate the use of SCIPs—particularly if regional licenses are awarded, because the majority of Public Safety Regions that FCC has proposed as the geographic regions are delineated along state lines.
- To help facilitate interoperability among federal agencies, the National Emergency Communications Plan outlines an initiative to implement the Advanced Encryption Standard for federal responders. FCC proposed no requirement that federal government agencies be provided access to the network and outlined no technical specification for the Advanced

[69]This is not intended to be an exhaustive list or proposal for how the 700 MHz Public/Private Partnership network could or should be aligned with the National Emergency Communications Plan or other DHS efforts. We also recognize that FCC has sought comment on aspects of its proposal and that a final order has not been issued. However, we believe that steps could be taken, as appropriate, to ensure that FCC's 700 MHZ Public Private Partnership plan, as adopted and implemented, is supportive of the National Emergency Communications Plan

[70]FCC officials noted that it was ineffectual to compare the strategic goals of the National Emergency Communications Plan to the performance benchmarks and build out requirements in the 700 MHz Public/Private Partnership proceeding. According to these officials, the plan is focused on improving the interoperability of current systems, while FCC's initiative would create a 100 percent interoperable network once built. Although we recognize the different emphasis, we continue to believe that FCC build out requirements could be leveraged to help meet the goals articulated in the National Emergency Communications Plan.

[71]According to FCC, it sought comments on a state role in coordinating participation in the network and received conflicting comments on these proposals.

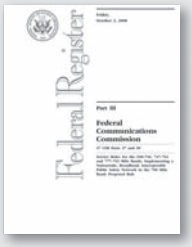
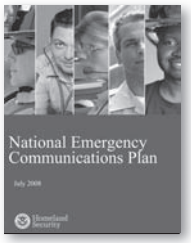
Encryption Standard.[72] Given that federal agencies play a key role during catastrophic events, if the 700 MHz network does not incorporate this standard,[73] it could pose a challenge for federal responders working with state and local responders on this network. The encryption of the network once built may not adhere to the Advanced Encryption Standard. Thus, if federal responders needed to share sensitive or classified information with one another or with local responders, this network might not be an option for them, since it may not meet their encryption standard. FCC could consider including this standard in the specifications for the network or ask the licensees to examine the consequences for not adhering to this standard and any potential remedies.

- FCC proposed that the network be based on a modern Internet Protocol platform and that interconnectivity through gateways and bridges be allowed. FCC officials told us that one of the key benefits of the network would be nationwide interoperability facilitated through this common technological architecture. According to DHS's Interoperability Continuum, though, interoperability is not the result of solely technological solutions. In order to achieve interoperability, other elements such as standard operating procedures, usage, governance, and training and exercises, must be addressed. FCC has not addressed these other elements. According to FCC officials, these facets of emergency communications fall under the purview of DHS and FCC has not contemplated requiring the licensee(s) to take any actions that would associate or connect the proposed network with DHS efforts. FCC officials also reported that historically, FCC has not taken such action within its rulemaking process. FCC could require that the licensees adopt use of DHS's Interoperability Continuum as a framework for negotiating the terms of the network sharing agreement (see fig. 14).

[72]In the Third Further Notice, FCC tentatively concluded that it would reaffirm its prior decision that it was the "sole discretion" of the public safety broadband licensee whether to permit federal public safety agency use of the public safety broadband spectrum. This decision was supported by NTIA in its comments filed to FCC.

[73]FCC mandated that the security and encryption be consistent with state of-the-art technology. However, because FCC did not expressly reference the Advanced Encryption Standard, it is unclear whether FCC's mandated encryption will adhere to the standard called for in the National Emergency Communications Plan.

Figure 14: Analysis of FCC's Third Further Notice and DHS Efforts

Opportunities for alignment	FCC 700 MHz Third Further Notice 	National Emergency Communications Plan and other DHS efforts 
Performance benchmarks and strategic goals	FCC requires the D Block licensee(s) to provide signal coverage and offer service to at least: • 40 percent of the population in each Public Safety Region by the end of the fourth year, • 75 percent by the end of the tenth year, and • D Block licensee(s) will be required to meet other benchmarks after 15 years.	The National Emergency Communications Plan has strategic goals that include: • 90 percent of all high-risk urban areas designated within the Urban Area Security Initiative are able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions by 2010, and • 75 percent of all jurisdictions are able to demonstrate response-level emergency communications within 3 hours, in the event of a significant incident as outlined in national planning scenarios by 2013.
Regional organization	58 Regional licenses designated by Public Safety Regions and one nationwide licensee (Public Safety Broadband Licensee) that would represent public safety in negotiating the network sharing agreement among other responsibilities.	10 DHS / FEMA Regional Emergency Communications Coordination Working Groups.
Role of state government	FCC proposed no specific role for state governments in coordinating their public safety providers' participation in the interoperable shared broadband network.	States have been instrumental in developing SCIPs, which are reviewed by DHS and NTIA and required by Congress to be eligible for federal emergency communications funding.
Federal agency access and encryption standard	FCC leaves access for federal agencies to the discretion of the Public Safety Broadband Licensee and outlines no technical specifications for the Advanced Encryption Standard.	Federal agencies will implement the Advanced Encryption Standard.
Interoperability	FCC interoperability through an Internet Protocol-based architecture.	DHS's SAFECOM Interoperability Continuum describes 5 elements for achieving interoperability: Governance, Standard Operating Procedures, Technology, Training and Exercises, and Usage.

Source: GAO analysis of FCC and DHS data.

The lack of commonly defined goals for the 700 MHz spectrum and mutually reinforcing strategies with DHS efforts threatens the usefulness and viability of the network for public safety. There is some support for a 700 MHz Public/Private Partnership to build a nationwide, interoperable broadband network from entities such as the Association of Public-Safety Communications Officials, but officials from major metropolitan areas, such as New York City, reported concerns with how the network will be governed, as proposed in the Third Further Notice. Specifically, the Deputy Chief from the New York City Police Department expressed

concern to FCC Commissioners in a July 2008 public hearing regarding a commercial vendor managing the network and said that his agency would likely not participate, because the network would not meet all their mission requirements.[74] First responders we met with in Boston, Seattle, and Sacramento expressed similar concerns about the proposed network. For example, Boston Police Department officials told us that based on their experience with commercial telecommunications providers and the proposed fees for using the network, they preferred to directly manage and control the spectrum's use in their jurisdiction. Should these and other jurisdictions not participate in the 700 MHz Public/Private Partnership's network, first responders in those areas would be left without access to a potentially vital resource during a catastrophic event, which is contrary to FCC's stated goals for the network.

DHS Could Leverage Emergency Communications Planning Expertise for Federal Agencies

As the federal government's lead agency on emergency communications, DHS has provided technical assistance and guidance on how to develop emergency communications plans, but these resources have primarily focused on state and local jurisdictions and less so on federal agencies. As previously discussed, DHS has provided extensive assistance to state and local jurisdictions in developing emergency communications plans, which have been valuable to state and local first responders in understanding their communications capabilities and limitations and working toward further enhancements. DHS has also issued guidance on emergency communications planning directed at all levels of government. For example, the National Preparedness Guidelines/Targeted Capabilities List, issued in September 2007, included 13 critical tasks for how to "Develop and Maintain Plans, Procedures, Programs, and Systems." DHS guidance outlines the importance and some key elements of emergency planning for preparedness and response, such as consideration of the systems that will be used, personnel (those who can use these systems), and other relevant considerations.

Not all federal agencies have developed communications plans or conducted communication infrastructure threat and vulnerability assessments, making their preparedness to assist state and local first

[74] *Public Hearing on Public Safety Interoperable Communications – The 700 MHz Band Proceeding*: Hearing Before the Federal Communications Commission (July 30, 2008). http://www.fcc.gov/realaudio/mt073008.ram, accessed April 2009.

responders uncertain.[75] According to the National Emergency Communications Plan, few agencies conduct communications infrastructure threat and vulnerability assessments as part of emergency communications planning on critical communications assets. As previously discussed, the National Communications Capabilities Report notes that some federal agencies currently have no formal plans in place to identify communications vulnerabilities or map a way forward to mitigate such vulnerabilities.

DHS has begun efforts that could assist other federal agencies, but it is unclear whether these will result in formal emergency communications plans. The National Emergency Communications Plan observes that some agencies do not view emergency communications planning as a priority and includes a milestone that by July 2009 DHS will develop "a standardized framework for identifying and assessing emergency communications capabilities nationwide." The plan also includes a milestone for DHS providing "best practices and methodologies that promote the incorporation of vulnerability assessments as part of emergency communications planning." Each federal agency and department should also assess its existing communications capabilities and compare them to the capabilities needed to complete each agency's missions. According to DHS officials, they are taking steps to help meet these milestones and to outreach and assist other federal agencies. However, it is too early to tell what direction these new efforts will take.

A formal emergency communications plan can help federal agencies respond in a catastrophic disaster by enhancing agencies' understanding of their emergency communications capabilities. Without such planning and understanding, federal agencies' fundamental readiness and response declines, including their ability to support state and local first responders in disaster. For example, FEMA Region IX officials reported that planning activities with various California jurisdictions have helped increase understanding on how FEMA will work and support California first responders, as well as achieving a common understanding of communications operations and assets. We have previously reported that limited emergency communications planning has reduced the federal government's readiness to support state and local first responders and

[75]It was beyond the scope of work for this engagement to assess the full extent of emergency communications planning completed by federal agencies. Not all federal agencies have communications infrastructure or the role/responsibility to assist state and local first responders with communications.

contributes to poor response. The Hurricane Katrina Lessons Learned Report highlighted that communications problems due to limited planning had a debilitating effect on response efforts in the Gulf Coast region.[76] Specifically, many available communications assets were not utilized fully because there was no national, statewide, or regional communications plan that incorporated them. According to a senior DHS official, agencies may find themselves at the center of response in certain disasters or other events, at which time communications weaknesses are revealed. Officials from federal agencies in our case studies, such as National Park Service officials at Mount Rainier and FBI officials, also reported the importance of emergency communications planning in preparedness and response to a catastrophic event. For example, FBI officials and local first responders in our Boston terrorism case study would be required to work closely together. According to a senior FBI official, a number of issues could interfere with the ability of FBI agents to carry out their duties, such as a lack of interoperability with local radio systems, inadequate encryption, and insufficient coverage.

Limited Monitoring May Impede Progress in Emergency Communications

We found that DHS and FCC had only limited processes in place to monitor and evaluate recommendations from stakeholder groups. We have previously reported that monitoring and evaluating efforts are crucial elements to achieving agency goals. Following up on stakeholder group recommendations could help key decision makers within the agencies to obtain feedback for improving both policy and operational effectiveness.[77] Instituting some of the recommendations these groups have made may improve emergency communications. For example, the National Coordination Committee, an advisory group set up by FCC, recommended that FCC require standard channel nomenclature for all interoperability channels in 2003.[78] During disaster response, it is crucial that all responding public safety agencies are able to tune their radios to the frequency or frequencies that the incident commander directs. However, there is little uniformity in the naming of radio channels—some responders designate

[76]U.S. Executive Office of the President, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, D.C.: February 2006).

[77]GAO/GGD-96-118.

[78]We have previously reported on the need for standard channel nomenclature to facilitate interoperability. GAO, *Homeland Security; Federal Leadership Needed to Facilitate Interoperable Communications among First Responders*, GAO-04-1057T (Washington, D.C.: September 2004).

their channels by colors, others by numbers. Standardized channel nomenclature could enhance interoperability, since responders across different jurisdictions and disciplines would use identical terminology for identifying radio frequencies, thereby minimizing confusion and delay. Standard channel nomenclature could prove particularly useful in catastrophic disaster response, because of the large numbers of responders from different jurisdictions and disciplines. According to the National Public Safety Telecommunications Council, FCC has not adopted this recommendation made in 2003. FCC officials reported that FCC made reference to this stakeholder group recommendation in a 2006 proceeding. FCC officials indicated that the recommendation was raised again in the ongoing 700 MHz Public/Private Partnership proceeding and that the recommendation would be addressed therein.

Without monitoring and evaluation, it is unclear how DHS and FCC have incorporated or kept pace with the work of their stakeholder groups. As previously discussed, the constantly evolving nature of emergency communications can create opportunities and challenges, some of which advisory groups have addressed. According to the National Public Safety Telecommunications Council, significant progress has been made in implementing recommendations that contribute to improved emergency communications, but meeting the demand for public safety communications is a dynamic process requiring ever-additional work. Our analysis revealed that stakeholder groups assembled by DHS and FCC have made some recommendations repeatedly that could address identified vulnerabilities (see fig. 15).[79]

[79]According to FCC officials, the agency is under no obligation to adopt any particular stakeholder group recommendation. Under the Federal Advisory Committee Act, the function of an advisory committee is to provide advice; a federal agency may implement or not implement an advisory committee's recommendation at its discretion.

Figure 15: Analysis of Advisory Group Recommendations 2004-2008

Vulnerability addressed	Recommendation	Year of recommendation				
		2004	2005	2006	2007	2008
Continuity of communications	Multiple access methods and alternative communication technologies, so that emergency communications are not disrupted	FCC				
				FCC		
				DHS		
					DHS	
					FCC	
	Emergency Responder Classification/ Credentialing for Telecommunications Provider			DHS		
				FCC		
					FCC	
	Pre-positioned or deployable communication assets, such as mobile radios and mobile cell towers for both public safety and commercial communications providers; related planning, training, and exercises.		FCC			
				FCC		
					FCC	
Capacity	Communication platforms capable of integrating different data types (voice, photos, etc.)	FCC				
					DHS	
						FCC
	Increased bandwidth to enable transmission of video and large format files such as blueprints and video files	FCC				
					DHS	
						FCC
Interoperability	Internet Protocol for an interoperable network of networks such as LMR, cellular, and wireline, which can also handle multiple services and applications	FCC				
			FCC			
					DHS	
						FCC
	Migration path from legacy systems to the Internet Protocol internetwork	FCC				
						FCC
	Develop Interoperability Rules to handle issues such as governance and prioritization	FCC				
					DHS	

Sources: GAO analysis of DHS and FCC stakeholder recommendations made in the following reports: Network Reliability and Interoperability Council VII reports #1 and #3; and Focus Group 1B National Security Telecommunications Advisory Committee Issue Review; FCC Hurricane Panel Order--Report Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks; National Security Telecommunications Advisory Committee Report to the President on Emergency Communications and Interoperability; and Joint Advisory Commitee on Communications Capabilities of Emergency Medical and Public Health Care Facilities Report to Congress.

Both agencies have various ways of examining some stakeholder group recommendations, but neither includes a mechanism to systematically monitor and evaluate all recommendations from stakeholder groups, or the agencies' response. As previously discussed, DHS's approach has been practitioner-driven. According to DHS officials, the agency tracks recommendations and input provided by its stakeholder groups in varying ways (see table 4).

Table 4: DHS Stakeholder Groups and Tracking Activities

DHS stakeholder group	Tracking activity
SAFECOM Executive Committee and Emergency Response Council	DHS tracks the recommendations and input provided by the SAFECOM Executive Committee (EC) and Emergency Response Council (ERC): • Formally through meeting reports • Informally through detailed minutes taken during biannual ERC meetings, monthly and quarterly EC conference calls, and face-to-face meetings, as well as during ad hoc working group meetings. • For biannual ERC meetings, DHS develops a formal meeting report, which documents the key content, input, and recommendations from the working sessions.

National Security Telecommunications Advisory Committee	The National Communications System (NCS), within DHS, tracks recommendations made by the National Security Telecommunications Advisory Committee (NSTAC). Once a recommendation is approved by the NSTAC, which is typically on a quarterly basis, DHS/NCS convenes a team of NCS managers and subject matter experts to determine what priority area the recommendations fall under and provides a quarterly
	status report to the NSTAC Chairperson on whether the recommendation will be:
	• Taken for NCS action; or
	• Closed because:
	  • There are insufficient resources;
	  • The recommendation is overcome by events;
	  • The recommendation is being addressed by another organization; or
	  • The NCS has completed its activities.

Federal Partnership for Interoperable Communications	Federal Partnership for Interoperable Communications (FPIC) standing committees (Interoperability, Security, Spectrum, and Standards) conducts the following activities: • Identify potential recommendations; • FPIC committee members draft recommendations and submit to the FPIC general membership for review and formal acceptance, if needed; and • Any member agency or advisory member that disagrees with a decision or vote of the FPIC may submit a Minority Report.

Source: GAO analysis of DHS information on a selection of stakeholder groups and tracking activities.

Not all these activities, however, result in the agency monitoring recommendations or evaluating its response. DHS's activities to monitor National Security Telecommunications Advisory Committee recommendations appear the most robust, as these mechanisms can account for which recommendations were acted upon and, if not, why. In contrast, though DHS tracking activities for its other stakeholder groups document recommendations and other information produced, DHS does not collect or record the agency's response.

FCC has not systematically monitored or evaluated recommendations of its advisory committees[80] and the agency's response, limiting the relevance of these groups' work. In December 2004, we reported that FCC did not have a process for tracking all its advisory committee recommendations. At the time, the deputy committee management officer told us that as a result of our review, FCC planned on improving the accountability of the advisory committee process by requiring committee recommendations be tracked.[81] To date, FCC has not established and instituted any such tracking mechanism. FCC officials reported that many of the recommendations from its advisory groups are not directed at FCC, and consequently, tracking or monitoring is less necessary. We note, in January 2009, the FCC Acting Chairman said that the agency could more fully take advantage of the work of advisory committees to increase agency transparency. FCC has tools at its disposal that it could use for monitoring and evaluating recommendations. For example, for its Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, FCC issued a Notice of Proposed Rulemaking (notice) in June 2006 inviting comment on what actions the Commission should take to address the Katrina Panel's recommendations.[82] FCC received over 100 comments and reply comments in response to the notice. On June 8, 2007, FCC released an order directing its Public Safety and Homeland Security Bureau to implement and track several of the recommendations that included FCC's rationale and conclusions behind selecting these particular recommendations (FCC Hurricane Panel Order).[83] The Public Safety and Homeland Security Bureau fulfilled the order by taking actions to implement the recommendations and reported to the commissioners after 3 and 9 months, as directed, on its actions.

[80]We have previously reported on the composition and transparency of federal advisory committee selection processes. GAO, *Issues Related to the Independence and Balance of Advisory Committees*, GAO-08-611T (Washington, D.C.: April 2008).

[81]GAO, *Federal Advisory Committees Follow Requirements, but FCC Should Improve Its Process for Appointing Committee Members*, GAO-05-36 (Washington, D.C.: December 2004).

[82]*Recommendations of the Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks*, Notice of Proposed Rulemaking, 21 FCC Rcd 7320 (2006).

[83]*Recommendations of the Independent Panel Reviewing the Impact of Hurricane on Communications Networks*, Order, 22 FCC Rcd 10541 (2007).

Both DHS and FCC are forming new stakeholder groups, but no mechanisms to monitor or evaluate these groups' work, or the agencies' response, are currently in place. Without such mechanisms, it will remain unclear how and to what extent federal agencies have considered, or incorporated, the information provided by these groups. For example, as previously discussed, FEMA has formed Regional Emergency Communications Coordination Working Groups across the country. However, while there are defined roles and responsibilities for these working groups in both the legislation and the National Emergency Communications Plan, there are no legislative requirements for DHS, FEMA, or any other agencies to monitor or evaluate information provided by working groups, such as recommendations or the agencies' responses. FCC is also supporting the development of a new advisory committee, the Communications Security, Reliability, and Interoperability Council. FCC filed the charter for the council with the appropriate House and Senate committees in April 2007.[84] The charter did not state if or how FCC will monitor, evaluate, or respond to the recommendations made by the council.[85]

Conclusions

For the first time, the National Emergency Communications Plan provides an overarching strategy for emergency communications at all levels of government. This plan and other significant federal efforts represent an increasingly strategic approach by the federal government to enhance emergency communications and address existing vulnerabilities. Collaboration and monitoring remain critical components for success given the complex nature of emergency communications, the number of stakeholders involved, and the numerous efforts underway. Those federal agencies that do not use collaboration best practices jeopardize the success of not only their own efforts, but those of other agencies who have a role in supporting and enhancing emergency communications. Identified emergency communications vulnerabilities may not only persist, but

[84]Although the Communications Security, Reliability, and Interoperability Council became technically operational the date the charter was filed, members were never determined and no meetings have been held. The charter was renewed on March 19, 2009, and the FCC recently issued a Public Notice seeking nominations for membership on the committee. According to FCC officials, the Network Reliability and Interoperability Council will be subsumed by the new Communications Security, Reliability, and Interoperability Council.

[85]The purpose of an advisory committee charter is to describe the mission, goals, and objectives of the advisory committee (41 CFR 102-3.75), and according to the FCC, the Communications Security, Reliability, and Interoperability Council charter fulfilled the relevant legal requirements.

deteriorate further as supporting infrastructure ages and technology continues to change. Establishing an effective governance structure by completing a MOU and establishing the Emergency Communications Preparedness Center would improve the implementation of efforts that depend on the participation of multiple agencies, such as the National Emergency Communications Plan. Other federal efforts, such as FCC's 700 MHz Public/Private Partnership proceeding would also benefit from DHS and FCC establishing a common vision and mutually reinforcing strategies. This would help the agencies speak with one voice as they work with state, local, tribal, and private stakeholders. Given DHS's past experience and expertise in leveraging resources to assist states with emergency communications planning, it is well suited to offer similar assistance to federal agencies. Such assistance would help ensure that agencies plan for an emergency response, including evaluating how their communications assets and capabilities could best assist state and local first responders in disaster. Like collaboration, monitoring is crucial for ensuring advancement of federal efforts to enhance emergency communication. Improved monitoring and accountability of stakeholder and advisory committees recommendations—including agencies considering, deciding, and acting on such recommendations—would boost the value of these groups by monitoring agency responses, avoiding duplication of efforts, and identifying opportunities to work with other agencies.

Ultimately, the success or failure of federal efforts to enhance emergency communications will have the greatest effect on state and local first responders. Vulnerabilities involving continuity of communications, capacity, and interoperability can all cause communications failures during catastrophic disasters. As in the past, when future catastrophic disasters cause similar failures, the federal government will play a vital role in response. Addressing vulnerabilities through successful collaboration and monitoring of the wide variety of ongoing federal efforts will be essential in determining the quality of this future federal assistance to overwhelmed state and local first responders.

Recommendations for Executive Action

We make four recommendations in this report to improve federal agencies' collaboration and monitoring in efforts related to emergency communications.

To help foster implementation of the National Emergency Communications Plan, we recommend that the Secretary of Homeland Security, in DHS's role as chair of the agency working group to establish the Emergency

Communications Preparedness Center, work to complete the MOU to establish the center. The MOU should include a clear purpose, expected outputs, and realistic performance measures from participating agencies.

To help ensure that DHS and FCC's significant emergency communications efforts, such as the National Emergency Communications Plan and the 700 MHz Public/Private Partnership, have a common vision and mutually reinforcing strategies, we recommend that the Secretary of Homeland Security and the Chair of the Federal Communications Commission establish a forum, or other mechanism, to better collaborate on each agency's emergency communications efforts. Such collaboration could identify opportunities for aligning agency activities to ensure that they are mutually reinforcing, as well as developing an action plan or other working document to develop a common vision for implementation of the National Emergency Communications Plan and its relationship to the future 700 MHz Public/Private Partnership.

To help ensure that federal agencies and their communications assets are well-positioned to support state and local first responders in catastrophic disasters, we recommend that the Secretary of Homeland Security provide guidance and technical assistance to federal agencies in developing formal emergency communications plans. These plans could include identifying how federal agencies' communications resources and assets will support state and local first responders in a disaster.

To help DHS and FCC enhance the value of stakeholder groups' recommendations, we recommend that the Secretary of Homeland Security and the Chair of the Federal Communications Commission systematically track, assess, and respond to stakeholder groups' recommendations, including identifying actions taken by the agencies in response to recommendations, whether recommendations are duplicative with past recommendations, and opportunities to work with other agencies, as appropriate, to advance recommendations.

Agency Comments

We provided a draft of this report to DHS, FCC, Commerce, Interior, and DOJ for official review and comment. In its comments, DHS generally agreed with our recommendations and noted that steps were already underway to implement some recommendations. Regarding our recommendation that DHS work to complete the Emergency Communications Preparedness Center's MOU, DHS stated that the agency had signed the MOU and that it had been circulated to the other interagency partners. While this represents progress, more work remains to complete

the MOU and reach consensus among agencies on its purpose, expected outputs, and performance measures. Regarding our recommendation that DHS and FCC establish a mechanism for better collaboration on emergency communication efforts, DHS stated that its Office of Emergency Communications had begun regular coordination meetings with FCC's Public Safety and Homeland Security Bureau to identify areas for collaboration and to work jointly on common solutions as appropriate. Regarding our recommendation on DHS providing guidance and technical assistance to federal agencies in developing formal emergency communications plans, DHS noted that the Homeland Security Act focuses on assistance to "state, regional, local, and tribal governments," providing limited authority for DHS to provide assistance to other federal agencies. We agree that DHS cannot compel agencies to work to develop formal emergency communications plans, but this recommendation would include DHS offering such assistance through guidance and making available its expertise to other agencies. Regarding our recommendation that DHS systematically track, assess, and respond to stakeholder groups' recommendations, DHS noted that its Office of Emergency Communications has worked closely with numerous stakeholder groups to track and use the information from these groups within its other emergency communications efforts, such as the development of the National Emergency Communications Plan. We agree that DHS has some measures in place to track, assess, and respond to some stakeholder groups, but our recommendation calls for such a process to be applied systematically to all stakeholder group recommendations.

FCC generally agreed with our recommendations and provided comments via e-mail that we summarize here. FCC said that most aspects of the recommendations are already being actively pursued by the FCC, DHS and other federal agencies. In addition, FCC said that it was engaged in a large amount of work that goes beyond the report's recommendations aimed at improving federal responses and eliminating vulnerabilities not addressed in the report. In its comments, FCC said that the report relies heavily on anecdotal information and opinion, which are often uncritically presented as representing objective truth. For example, FCC questioned the use of several interviews with state and local officials about communications vulnerabilities forming the basis for much of the discussion of vulnerabilities in the report. As presented in our objectives, scope, and methodology, our case study work and related interviews were one component of identifying vulnerabilities. We also conducted a literature review of prior GAO products and other agency reports on emergency communications to ascertain and analyze common vulnerabilities.

Furthermore, the three primary vulnerabilities that we identified are similar to vulnerabilities identified by DHS, FCC, and other stakeholder groups.

FCC said that the report also lacks a sufficient number of facts about vulnerabilities, meaning that there will be no adequate way to judge whether the adoption of the recommendations actually improves emergency communications. Furthermore, FCC said that the report identifies vulnerabilities, but does not place them in context or suggest priorities in terms of how they should be addressed. As stated in our report, our recommendations will help federal efforts in addressing challenges to improve emergency communications by helping foster implementation of the National Emergency Communications Plan, helping ensure that significant emergency communications efforts share a common vision and have mutually reinforcing strategies, helping ensure that federal agencies and their communications assets are well-positioned to support state and local first responders, and by helping DHS and FCC enhance the value of stakeholder groups' recommendations. In addition, ranking, prioritizing, or suggesting how to address the vulnerabilities, was outside the scope of our work. We collected information from local and state emergency managers, law enforcement, firefighters, and other first responders, as well as federal officials and telecommunications industry officials, on efforts to address some of these vulnerabilities. We include this information on what jurisdictions are doing to address vulnerabilities throughout our report. Furthermore, our identification of vulnerabilities does not preclude FCC or another organization from exploring metrics or other benchmarks to track progress in addressing these vulnerabilities.

FCC also said that it was unclear whether the report is intended to address only first responder communications or all types of emergency communications, including commercial communications. We have clarified in our report that unless otherwise noted, when we refer to emergency communications systems, we mean those systems used by first responders. FCC also said that the report overlooks many vital issues, such as all the collaborative work done by federal agencies and communications companies to prepare and respond to communications disasters. We disagree that we omitted all collaborative work done by federal agencies and communications companies. We acknowledge in the report that DHS and other federal agencies have recently taken significant and strategic steps to enhance emergency communications and that a range of other federal efforts are underway. Additionally, we interviewed telecommunications industry officials as part of our audit work, and reported on the communications assets that companies can provide. Furthermore, we reported that private stakeholders, such as

telecommunications companies and equipment manufacturers, have invested heavily to develop innovative technological solutions and expand or strengthen their networks for emergency responders and commercial use. We did not intend our report to include or highlight all technological capabilities present in certain emergency communications systems. We made changes to clarify the scope of our work, but remain confident about our findings and conclusions.

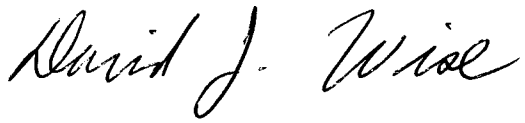
In its comments, Commerce provided information on two of its agencies'—NOAA and NTIA—roles in emergency communications. Commerce commented that emergency communications are important and that federal agencies must effectively coordinate to mitigate vulnerabilities. In its comments, Interior said that the report could have been improved if it incorporated Interior or federal interoperability collaboration efforts in regards to emergency response capabilities based on the following. First, we could have expanded the report's geographic scope such as including a case study involving fire. We do not intend to understate fire hazards by not including a fire scenario. However, our case studies represent a variety of different disaster scenarios representing different regions of the United States and we do not imply that these are the only possible catastrophic disaster scenarios. Interior said that we also could have conducted interviews with Interior's Emergency Management Offices. While we report on several federal efforts involving emergency communications, our examples do not constitute a complete list, or evaluation of the effectiveness of federal assistance currently available to first responders. Interior also said that the team could have reviewed existing emergency deployment systems capabilities and nationally recognized emergency and day-to-day interoperability efforts throughout the United States. Our work included conducting interviews with first responders and federal officials across the country and receiving information on communications capabilities and efforts to improve interoperability, among other things. DOJ did not provide comments on our draft report. DHS, FCC, Commerce, and Interior also provided technical comments that we then incorporated, where appropriate. DHS's, Commerce's, and Interior's letters are contained in appendices V, VI, and VII respectively.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Secretary of Homeland Security, the Chair of FCC, the Secretary of Commerce, the Attorney General, the Secretary of the Interior, and appropriate

congressional committees. In addition, the report is available at no charge on GAO's Web site at http://www.gao.gov.

If you have any questions concerning this report, please contact me on (202) 512-2834 or wised@gao.gov. Contact points for our offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VIII.

Sincerely yours,



David J. Wise
Director, Physical Infrastructure Issues

Appendix I: Objectives, Scope, and Methodology

The objective of this report is to provide information on the status of emergency communications used by first responders. In particular, we sought to identify (1) vulnerabilities, if any, to emergency communication systems; (2) federal assistance available or planned to first responders for addressing any vulnerabilities or enhancing emergency communications; and (3) challenges, if any, with federal emergency communications efforts.

To identify vulnerabilities, if any, to emergency communication systems, we developed six case studies and subsequent analyses of varying catastrophic disaster scenarios both natural and man-made. In its National Response Framework, the Department of Homeland Security (DHS) defines catastrophic disasters as any natural or man-made incident that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.[1] Further, GAO has defined catastrophic disasters as a disaster whose effects almost immediately overwhelm the response capacities of affected state and local first responders and require outside action and support from the federal government and other entities.[2] The scenarios captured by our case studies contain elements from both of these definitions of catastrophic disasters.

Our case studies included a flood in northern California, a hurricane in southern Florida, a tsunami in Hawaii, a terrorist attack in Massachusetts, an earthquake in Tennessee, and a volcanic mudflow in the state of Washington. With this selection, we do not mean to imply that these are the only possible catastrophic disaster scenarios. The first step in selecting our particular case studies was to identify an exhaustive list of disaster scenarios facing communities across the United States. We limited this search to states, including Alaska and Hawaii. We conferred with subject matter experts, and reviewed data and documents from sources such as National Oceanic and Atmospheric Administration (NOAA), United States Geological Survey (USGS), and nongovernmental entities to produce a preliminary list of potential case studies. After producing our initial list of over 60 potential scenarios, we compared this list to available Geographic

[1]Department of Homeland Security, *National Response Framework* (Washington, D.C.: January 2008).

[2]GAO, *Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System*, GAO-06-618 (Washington, D.C.: Sept. 6, 2006).

Information Systems (GIS) data, which ranked metropolitan areas by the types of hazards they face (i.e., seismic hazards, historic hurricane strikes, etc.). This GIS data included historical disasters from 1980 to 2006.[3] We also consulted USGS, NOAA, and other documents on historically less frequent disasters that could occur in our lifetimes. We identified overlap with our initial list and formulated several criteria to help select our final set of case studies. Our criteria included:

- National level impact—We selected scenarios that would have far-reaching impacts beyond the immediate location of the disaster. Responding to such disasters would be beyond the capacity of state and local officials, requiring assistance from the federal government.
- Likelihood of occurrence—We selected scenarios that had a higher likelihood of occurrence within our lifetime.
- Potential fatalities and injuries—We considered the population of scenario areas, as well as related casualty forecasts, models, and expert opinions to select scenarios that were more likely to cause higher numbers of fatalities and injuries.
- Economic impact—We considered potential economic losses, including damage to public and private infrastructure and the loss of public and private revenue.
- Diversity of catastrophic disaster—We selected a variety of scenario types to show how different disasters (i.e., earthquakes, hurricanes, tsunamis, and volcanic mudflows) may pose similar and/or different challenges to emergency communications systems.
- Diversity of geography—We selected scenarios to represent different regions of the United States.

Data were not available to fully evaluate all scenarios under our criteria. Previous research has not calculated estimated economic or other financial losses for all of our scenarios beyond a broad range (i.e., in the tens of billions). Also, we included one of our case studies, a terrorist attack in Boston, given continued high interest in terrorism by Congress and first responders. This case study did not directly follow our selection method for the other five, although some of the same criteria—such as

[3]The GIS data did not include tsunami hazards. We consulted other data and included Honolulu, Hawaii (as well as other population centers in Hawaii) for several reasons. These included the example of the catastrophic tsunami that hit Indonesia in 2005, tsunamis repeatedly striking Hawaii over the past century, and the unique challenge of Hawaii's relative geographic isolation to the U.S. mainland.

potential fatalities and injuries, economic impact, and diversity of geography—still apply. Other criteria, such as likelihood of occurrence, have less application regarding the location of another terrorist attack. We selected Boston, Massachusetts, as the location of our terrorism scenario because it is among the top 20 population centers in the United States and is located in the Northeast, a region not represented by any of our other case studies. Furthermore, two of the planes involved in the September 11, 2001, terrorist attacks flew out of Boston's Logan International Airport. To provide context for a catastrophic terrorist attack, we used the Homeland Security Council's Planning Scenario Document.[4] This document provides 15 all-hazards planning scenarios for use in national, federal, state, and local homeland security preparedness activities. These scenarios are designed to be the foundational structure for the development of national preparedness standards. Because our criteria included physical damage to communications systems, we used the Council's scenario involving a nuclear detonation of a 10-kiloton improvised device. When meeting with state and local stakeholders for this scenario, we described details of this catastrophic disaster.

In developing our case studies, we visited site locations and interviewed local and state emergency managers; law enforcement, firefighters, and other first responders; and regional federal officials to help identify emergency communications vulnerabilities. We discussed catastrophic scenarios particular to each case study location and toured federal, state, and local emergency facilities. First responders also demonstrated available emergency communications equipment. We provide additional information on the hazards associated with each case study in appendix II. We conducted summary analyses of interviews and other information that we collected on these site visits. In addition to our case studies, we also conducted a literature review of prior GAO products and other agency reports on emergency communications to ascertain and analyze common vulnerabilities. The three primary vulnerabilities to emergency communications that we identified are similar to vulnerabilities identified by DHS, the Federal Communications Commission (FCC), and other stakeholder groups.

[4]Homeland Security Council, *Planning Scenarios – Executive Summaries*, Version 2.0 (Washington, D.C.: July 2004). We also used this document to provide context for some of our other scenarios, such as the effects of major hurricanes and earthquakes.

To identify federal assistance available to first responders for emergency communications, we interviewed officials and reviewed program documents from a variety of federal agencies with communications responsibilities and efforts underway or planned. Our work focused on the availability of federal assistance, but did not include a comprehensive evaluation of the effectiveness of this assistance. We reviewed recent emergency communications strategic guidance and documents from agencies such as DHS, FCC, and DOJ. We also reviewed FCC's 700 MHz Public/Private Partnership proceeding. Our work included a review of key planning documents such as the National Emergency Communications Plan. We also reviewed provisions of the Post-Katrina Act to identify new efforts underway to meet the act's emergency communications requirements. To obtain information regarding emergency communications grants and funding available to state and local first responders, we interviewed FEMA officials in the Grant Programs Directorate, as well as DOJ officials involved with law enforcement grants involving funding for emergency communications. To identify technical support, initiatives, and assets available to first responders in advance of or during a catastrophic disaster, we interviewed DHS and DOJ officials, and reviewed our recent work on several agency efforts. We also gathered information on available federal assistance during our case study work, collecting examples of state and local first responders' experiences and perceptions of federal guidance, grants, and other efforts.

To identify and examine any challenges with federal efforts to enhance emergency communications, we consulted our past work on emergency communications, interagency collaboration, and federal government program management and performance. Based on this review, we selected several best practices in collaboration—including establishing a common goal, developing mutually reinforcing strategies, and leveraging resources—and for government accountability and program performance relevant to emergency communications. We collected and analyzed key federal agency documents, such as DHS's National Emergency Communications Plan, National Communications Capabilities Report, National Preparedness Guidelines, FCC's notices for proposed rulemaking in the 700 MHz Public/Private Partnership proceeding, and other publicly available documents, such as comments filed to FCC from public safety entities. We determined the extent of interagency collaboration with regard to some significant federal efforts by comparing these efforts as described within these key agency documents, interviews with federal officials, state and local responders, and others against our selected best practices in collaboration. To determine the extent of monitoring being conducted by federal agencies of stakeholder groups' recommendations,

we analyzed recommendations issued over the past 5 years to identify those which were repeatedly made and relevant to the vulnerabilities we identified. Additionally, we interviewed federal agency officials on what steps their respective agencies had taken to collaborate and monitor federal efforts, such as the Emergency Communications Preparedness Center and the National Emergency Communications Plan. We also interviewed state and local first responders, professional and trade group representatives, and telecommunications industry officials and reviewed testimony provided by these groups before Congress and FCC to obtain their perspectives on challenges to federal efforts.

We conducted this performance audit from February 2008 to May 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Case Study Disaster Scenarios

The following provides additional background information and context on the hazards associated with each of our case study locations. These case studies included a flood in northern California, a hurricane in southern Florida, a tsunami in Hawaii, a terrorist attack in Massachusetts, an earthquake in Tennessee, and a volcanic mudflow in the state of Washington. The scenarios are hypothetical and we include descriptions of potential impacts, including the geographic area and populations affected, event frequency, hazards descriptions, and maps depicting a particular hazard on a national scale.

Sacramento Flooding

Disaster Type

A large flood in the city of Sacramento, California, and the surrounding Central Valley.

Geographic Area and Populations Affected

The city of Sacramento, the California state capital, is located in the Central Valley, which encompasses the floodplains of two major rivers—the Sacramento and the San Joaquin—as well as additional rivers and tributaries that drain from the Sierra Nevada Mountains. The approximately 1.8 million residents of Sacramento and the surrounding Central Valley would feel the most significant and direct effects of flooding. However, widespread flooding would likely have effects on the entire state of California by disrupting the state government (Sacramento's Capitol Building is below the flood water level), utilities, and drinking water. The Sacramento area provides two-thirds of the drinking water to Southern California.

Event Frequency

The actual number of years between floods of any given size varies greatly. Severe floods can occur in successive or nearly successive years. Scientists observe how frequently different sizes of floods occur, and the average number of years between them, to determine the probability that a flood of any given size will be equaled or exceeded during any year.

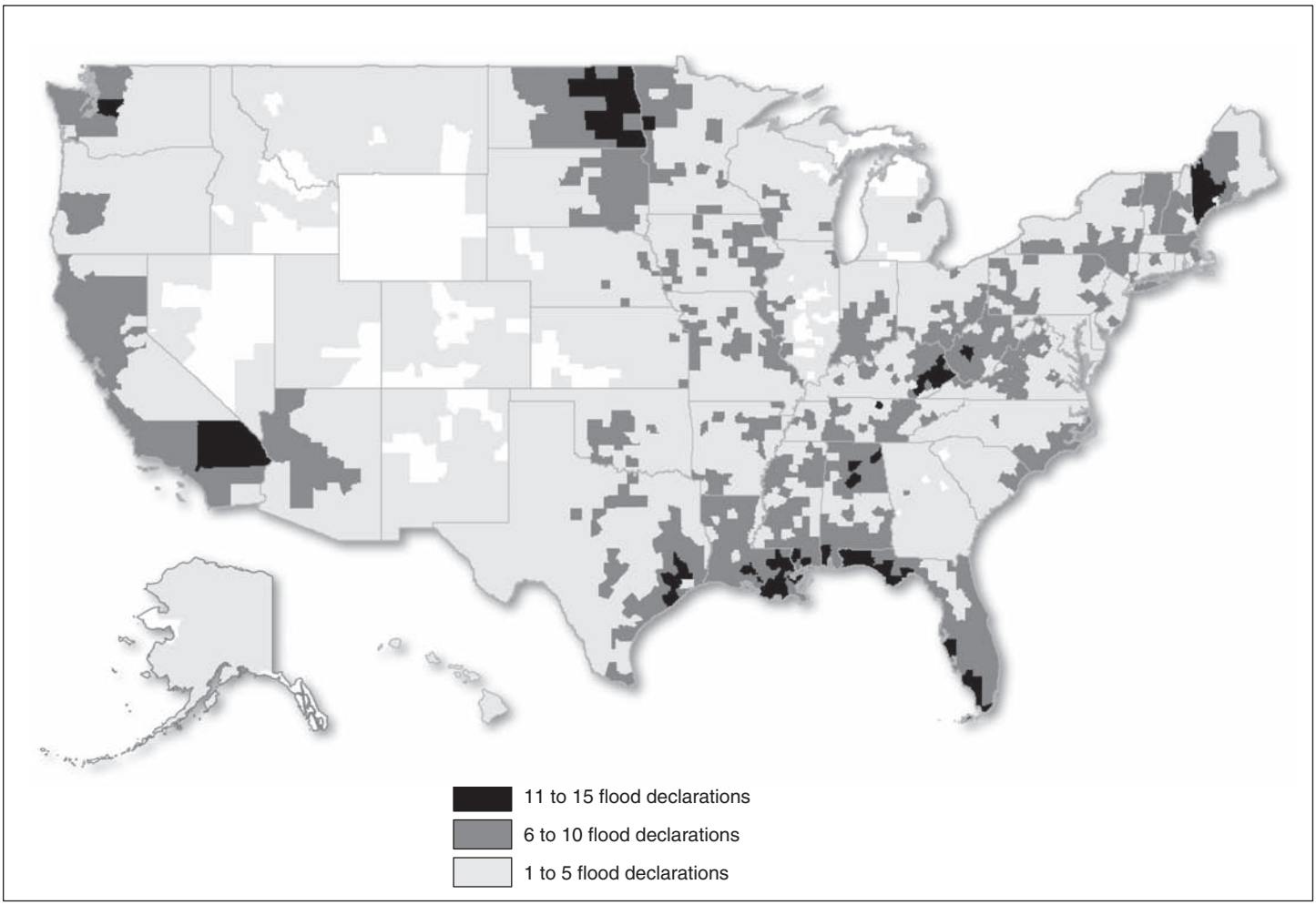
- A 100-year flood has water levels high enough that there is a 1 percent chance of being equaled or exceeded in any given year.
- A 500-year flood has water levels high enough that there is a 0.2 percent chance of being equaled or exceeded in any given year. Since 1951, the Sacramento area has experienced five major floods (see fig. 16 for a national map of flood declarations since 1980).

Hazards Description

- **Extensive flood zones:** There are three different types of flood events in the Sacramento area: flash, riverine, and urban storm water.[1] Flash floods are localized and the result of extensive rainfall. Riverine floods occur when riverbeds overflow into the flood zone. Existing flood zones in Sacramento County are extensive. Urban storm water floods result when urban drainage systems cannot handle the quantity of runoff from rainfall.
- **Aging infrastructure might fail:** The Central Valley's aging flood-control system provides only limited protection as many of the system's levees were poorly built or placed on top of older foundations up to 150 years old. Several areas of the county are subject to flooding by the overtopping of rivers and creeks, levee failures, and the failure of urban drainage systems to accommodate large volumes of water during severe rainstorms.
- **Other natural disasters can cause flooding:** While heavy rains are a major factor contributing to flooding, a major earthquake in the Bay Area could also destroy levies, which would result in massive flooding in the Sacramento area.

[1]Sacramento County Hazard Identification, Multi-Hazard Mitigation Plan (December 2004).

Figure 16: Number of Major Flood Declarations by County, 1980 - 2005



Sources: GAO analysis of Federal Emergency Management Agency (FEMA) data; Map Resources (map).

Miami Hurricane

Disaster Type

Major hurricane striking southern Florida near the City of Miami.

Geographic Area and Populations Affected

A hurricane is a tropical cyclone storm system, which generally forms in waters with temperatures at or above 80 degrees Fahrenheit, such as those off of the U.S. coastlines in the Gulf of Mexico and Atlantic Ocean. A major hurricane striking the coast of Florida near the City of Miami and surrounding Miami-Dade County would bring high winds, heavy rains, and ecological damage to an area with approximately 2.4 million people. The effects of a major hurricane can include power and water outages, damage to buildings and roads, and restricted communication and rescue operations in the 24 hours following the storm.

Event Frequency

- "Hurricane season" is from June 1 through November 30. According to a NOAA official at the Tropical Prediction Center, August to October is the time of highest risk for hurricanes for southern Florida.
- Hurricane intensity is measured on the Saffir-Simpson hurricane scale, which classifies hurricanes on a scale of 1 to 5, based on the sustained wind speed. A category 1 hurricane has sustained winds of 74 to 95 miles per hour, while a category 5 has sustained winds greater than 155 miles per hour. A category 4 hurricane (storms with sustained winds of 131 to 155 miles per hour) or stronger hurricane hits southern Florida every 16 years. (See fig. 17 for a national map showing the location and number of hurricane strikes, including southern Florida, since 1980.)

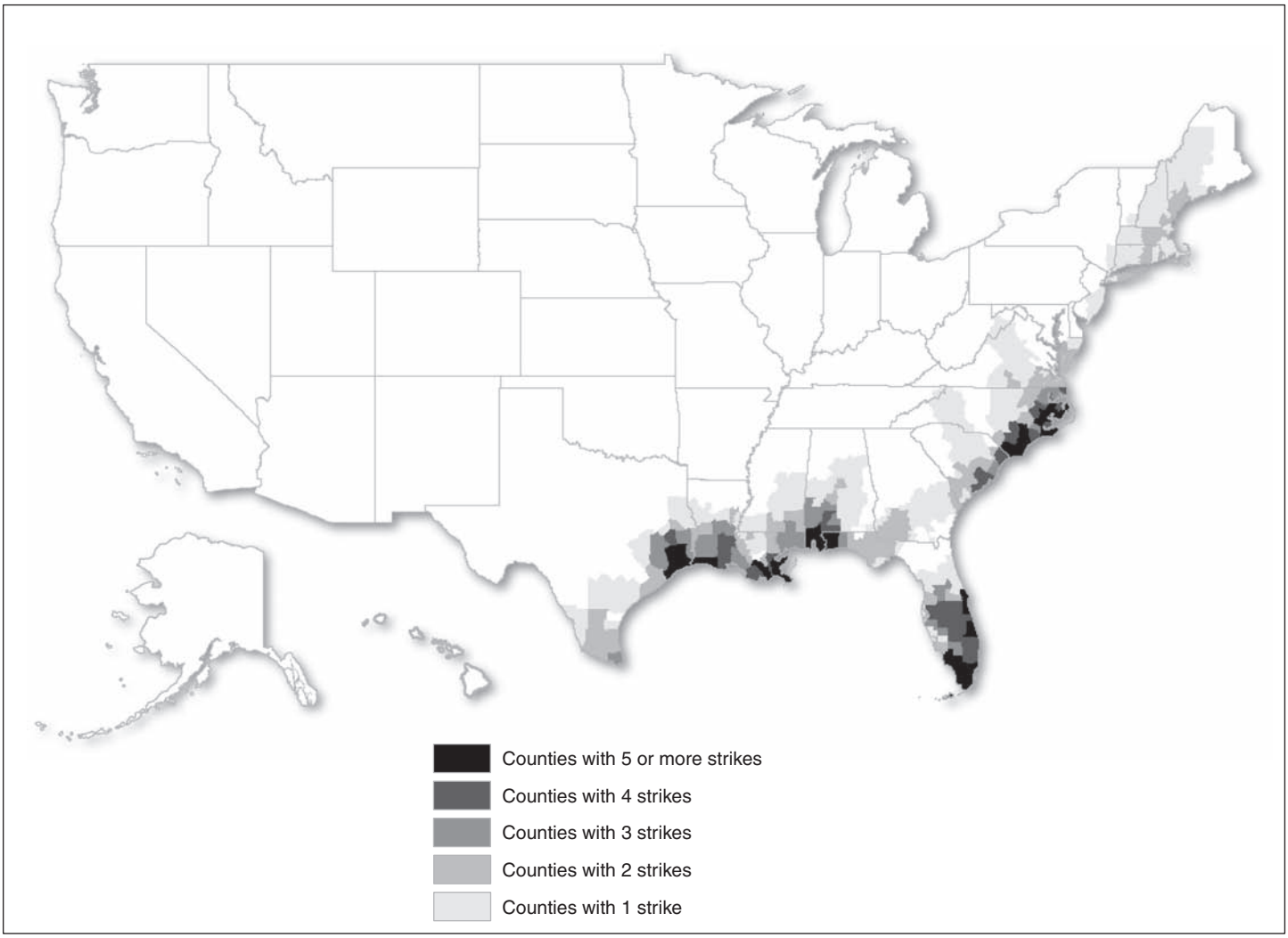
Hazards Description

- **High Winds:** Hurricane-force winds can destroy constructed buildings and mobile homes. Debris such as signs, roofing material, and items left outside can become airborne in hurricanes. Downed trees and other debris, such as occurred when Hurricane Andrew struck southern Florida in 1992, would largely restrict movement, including aid, for the first few days. Local building codes account for and are designed to withstand high winds from moderately strong hurricanes, however, buildings are likely to suffer power and water outages, as well as have windows destroyed, potentially making them uninhabitable. A category 5 hurricane would test even these building codes, the most stringent in the nation for hurricanes.
- **Storm surge:** Water that is pushed toward the shore by the force of the winds swirling around the storm (the storm surge) combines with wave action and the normal tides to push water onshore to depths of as much as 15 feet or more. According to NOAA officials, these waters would penetrate inland at decreasing depths over eastern sections of Miami near the waterfront. They could extend even further inland up rivers.
- **Inland flooding:** According to NOAA officials, for the 35 years preceding Hurricane Katrina's landfall along the Gulf Coast, inland flooding was

responsible for more than half the deaths associated with domestic hurricanes. While the City of Miami is less vulnerable than New Orleans (it is not situated below sea level), sections of the city have been flooded by rainfall associated with major hurricanes and weaker tropical cyclones.

- **Associated Tornadoes:** Hurricanes can also produce tornadoes, adding to the potential for destruction.

Figure 17: Number of Hurricane Strikes by County, 1980 - 2007



Sources: GAO analysis of National Oceanic and Atmospheric Administration (NOAA) data; Map Resources (map).

Honolulu/Hilo Tsunami

Disaster Type

A tsunami striking coastal communities in the state of Hawaii, including Hilo on the island of Hawaii and Honolulu on the island of Oahu.

Geographic Area and Populations Affected

Coastal communities in Hawaii are at high risk for tsunamis. Tsunamis potentially destructive to Hawaiian communities, including the cities of Hilo and Honolulu, may originate at distant locations around the perimeter of the Pacific Ocean, or may be locally generated by earthquakes on or near Hawaii. A tsunami originating in Alaska's Aleutian Islands would reach the Hawaiian Islands in 4.5 to 5.5 hours.

Event Frequency

- About 50 tsunamis have occurred in Hawaii since the early 1800s. Seven of these tsunamis caused major damage to Hawaii, and two of these tsunamis were locally generated near Hawaii. One of the most severe occurred in 1946 when a tsunami originating in the Aleutian Islands struck Hawaii without warning and killed over 170 people.[2]
- According to NOAA officials, Hawaii has a high risk for future tsunamis given its location in the middle of the Pacific Ocean, where about 80 percent of all recorded tsunamis have occurred.
- NOAA officials also reported that tsunamis hit Hawaii several times per century. It has been 34 years since the last tsunami struck Hawaii in 1975. (See fig. 18 for a map of high and very high hazard coastal areas based on tsunami frequency.)

Hazards Description

- **Different triggers:** Tsunamis are large, rapidly moving ocean waves triggered by a major disturbance of the ocean floor—typically an earthquake—but sometimes by a sub-marine landslide or volcanic eruption. A tsunami wave can travel at speeds of 600 miles per hour.
- **Little to no warning:** Locally generated tsunamis are potentially the most dangerous, because the time between their generation and when the

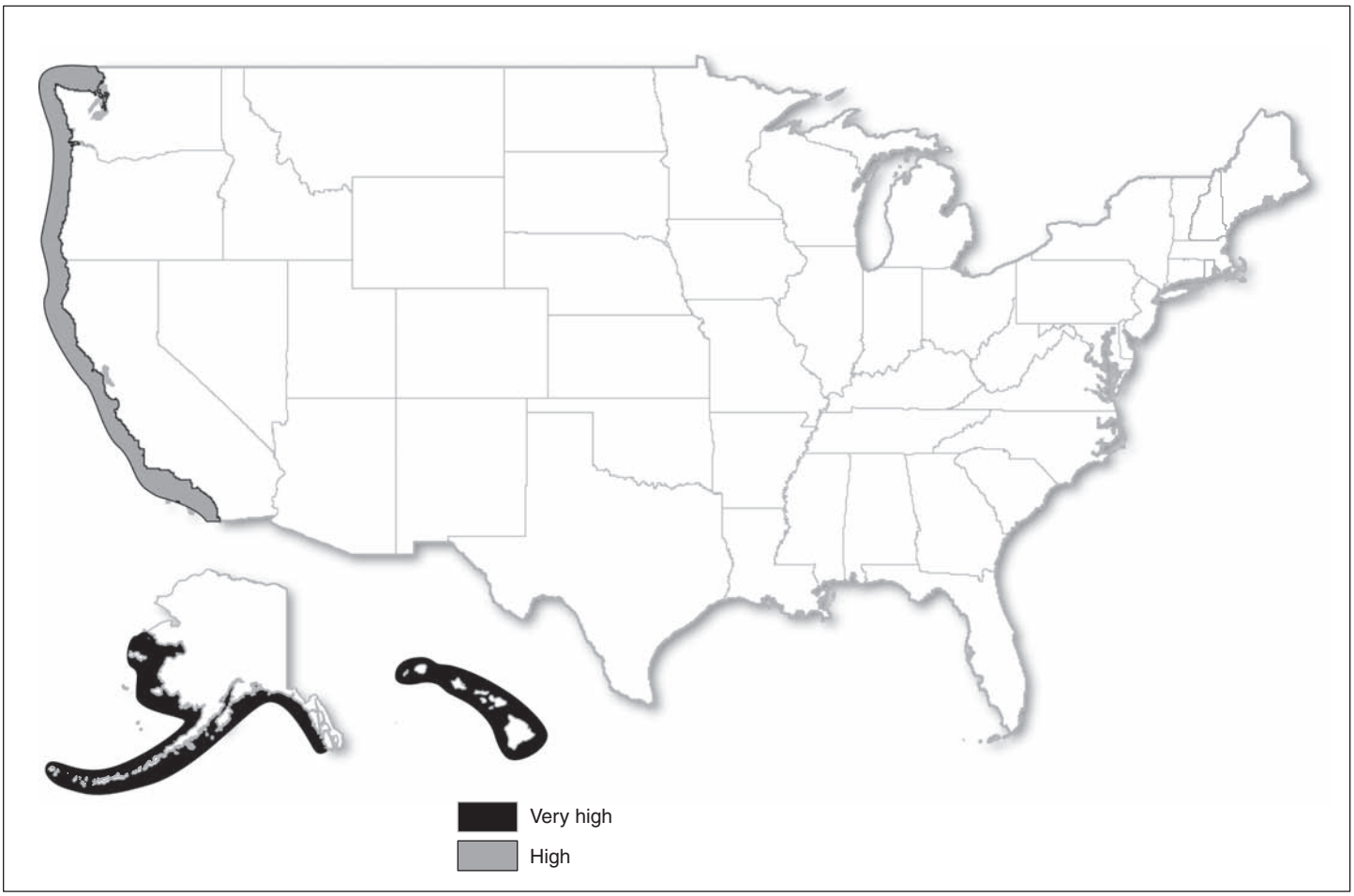
[2]Following the 1946 tsunami, a tsunami warning system for the Pacific basin was developed. Presently, the Pacific Tsunami Warning Center System, which has its headquarters in Honolulu, is administered by the National Weather Service under NOAA.

waves arrive on shorelines may be too brief to warn and evacuate people. After an earthquake near Hawaii in 1975, the first wave reached Hilo 20 minutes later. Distant tsunamis generally take hours to arrive, which would allow more time for evacuation.

- **Wave Damage:** As the tsunami approaches the coast, the wave speed slows as the wave height grows in the shallower waters, sometimes cresting at heights of 100 feet and striking the land at speeds of 30 mph or above. A series of waves may strike a coastline at intervals of every 5 to 40 minutes, and the first wave is often not the largest.[3] The size and destructiveness of the waves are largely determined by the local topography, both onshore and offshore, and the direction from which the wave approaches. A tsunami wave may be very small in the deep ocean, but can become a fast-moving wall of turbulent water as it approaches land.

[3]*U.S. Tsunami Preparedness: Federal and State Partners Collaborate to Help Communities Reduce Potential Impacts, but Significant Challenges Remain*, GAO-06-519 (Washington D.C.: June 2006).

Figure 18: Tsunami Hazard Based on Frequency



Sources: GAO analysis of National Oceanic and Atmospheric Administration (NOAA) data; Map Resources (map).

Boston Terrorist Attack

Disaster Type

Terrorist incident involving the detonation of a 10-kiloton improvised nuclear device in Boston, Massachusetts.[4]

Geographic Area and Populations Affected

A nuclear bomb blast in a major metropolitan area such as Boston would cause widespread casualties, damage, and economic disruption. Approximately 600,000 people reside in the city of Boston, and over 3 million people live in the greater metropolitan area. The most severe effect of a 10-kiloton nuclear device would be felt within a few miles of the detonation point. Flying debris may damage areas within approximately 3.5 miles of the detonation point. Severe radiation fallout can cause acute health hazards up to 150 miles from point of detonation, and less severe radiation can cause contamination up to 3,000 miles from point of detonation.

Event Frequency

The likelihood of a terrorist attack is unknown; however, DHS has determined the Boston area to be at risk of attack and has designated it as an Urban Areas Security Initiative region. The criteria to determine the risk to urban areas includes and considers threats, vulnerabilities and consequences, such as threats from international terrorist networks and their affiliates (see fig. 19 for a national map of these regions).[5]

Hazards Description

- **Detonation zone:** The intense heat of a nuclear explosion produces fires located throughout the immediate blast zone. Human casualties, damaged buildings, downed power and phone lines, leaking gas lines, broken water mains, and weakened bridges and tunnels are just some of the hazardous conditions that could result. If industrial storage facilities and manufacturing operations are located near the detonation site, additional hazardous materials could also be released.

[4]Homeland Security Council, *Planning Scenarios – Executive Summaries, Version 2.0* (Washington, D.C.: July 2004).

[5]*Homeland Security: DHS Risk-Based Grant Methodology Is Reasonable, But Current Version's Measure of Vulnerability Is Limited*, GAO-08-852 (Washington D.C.: June 2008).

- **Electro-magnetic pulse:** A nuclear explosion could also produce a high-voltage spike called an electro-magnetic pulse. This pulse radiates outwards from the detonation site and has the potential to disrupt the communications network, other electronic equipment, and associated systems within an approximately 3-mile range from the detonation point.
- **Damage to infrastructure:** There could be significant damage to general infrastructure, including transportation systems, power generation and distribution systems, communications systems, food distribution, and fuel storage and distribution. There could also be concerns about the safety and reliability of structures such as dams and hazardous material storage facilities. Structures that provide essential services, such as hospitals and schools, may also be damaged.
- **Radiation fallout:** The effects of the damage from the blast, radiation, and fallout could be significant within an approximately 3-mile range of the detonation point, with lesser effects on populations up to 3,000 miles away.

Figure 19: Urban Areas Security Initiative Regions, 2008

Sources: GAO analysis of Federal Emergency Management Administration (FEMA) data; Map Resources (map).

Memphis Earthquake

Disaster Type

Major earthquake in the New Madrid seismic zone near Memphis, Tennessee.

Geographic Area and Populations Affected

The New Madrid Seismic Zone is a collection of fault lines in the central United States. An earthquake in the New Madrid Seismic Zone earthquake

could shake the entire Mississippi Valley, including the states of Tennessee, Missouri, Arkansas, Mississippi, Illinois, Kentucky, and Ohio. This area is home to millions of people and includes the cities of St. Louis, Missouri; and Memphis, Tennessee.

Event Frequency

- The zone has produced several major earthquakes since 1800 and geologists expect similar earthquakes in the future.[6] Geologists have dated evidence of past earthquakes at or exceeding 7 in magnitude to the years 900 and 1450.[7] This suggests that magnitude 7 or greater earthquakes reoccur in the region approximately every 500 years. The last series of 7 or greater earthquakes was in 1811-1812 (see fig. 20 for a national map of earthquake hazards). The last earthquake over magnitude 6 in the New Madrid seismic zone was a 6.6 tremor in 1895.
- USGS has calculated the probability of a damaging earthquake of magnitude 6 or greater in the region to be between 25 to 40 percent in the next 50 years.

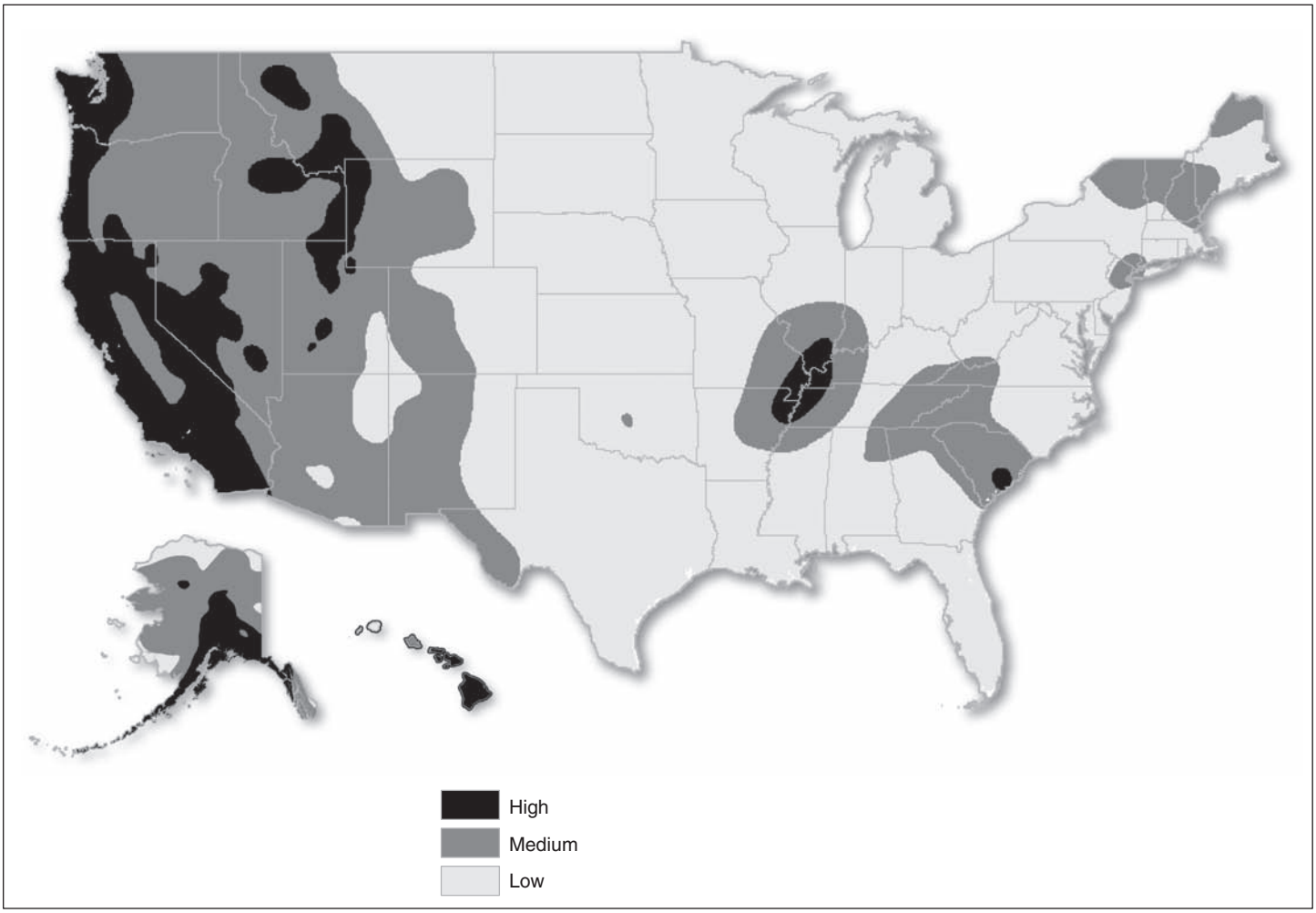
[6]U.S. Geological Survey Fact Sheet FS-131-02 (October 2002).

[7]Earthquake magnitude is a measure of the size of an earthquake and is based on ground motions recorded on seismographs.

Hazards Description

- **Seismic waves:** Seismic wave energy decreases much more slowly in soils in the central and eastern United States than in western portions of the country. Consequently, there could be shaking over a larger area.
- **Unstable soil:** Muddy, sandy deposits found near rivers tend to liquefy during an earthquake, which causes buildings to sink, tip over, and otherwise destabilize.
- **Damage to infrastructure:** Potential losses from a major earthquake are expected to be significant due to buildings not designed and constructed to withstand strong shaking. A quake will most likely damage businesses, transportation, communication, oil and natural gas pipelines, and housing.
- **Economic losses:** Estimated building damage costs could run as high as $70 billion from one major earthquake alone. Economic costs from disruptions in commerce through the center of the country could cost additional billions.

Figure 20: High, Medium, and Low Seismic Hazards



Sources: GAO analysis of United States Geological Survey (USGS) data; Map Resources (map).

Mount Rainier Volcanic Mudflow

Disaster Type

A volcanic mudflow, also called a "lahar", descending from Mount Rainier and inundating communities in Washington state.

Geographic Area and Populations Affected

A major lahar originating from Mount Rainier in Washington state could inundate portions of the Puget Sound lowlands, including the towns of Orting, Puyallup, as well as portions of the city of Tacoma over 40 miles from the mountain's summit. Research indicates that Mount Rainier has been the source of many lahars that buried areas that are now densely populated.[8]

Event Frequency

- During the past few thousand years, lahars reaching the Puget Sound lowlands have occurred every 500 to 1,000 years. The last lahar to reach the Puget Sound lowlands occurred approximately 500 years ago. Past lahars have struck different areas in the vicinity of Mount Rainier. For example, during the last lahar to reach the Puget Sound lowlands approximately 500 years ago, the lahar did not inundate the present location of the city of Tacoma.
- Smaller flows not extending as far as the Puget Sound lowlands occur more frequently. USGS estimates at least a one in seven chance of a lahar reaching the Puget Sound lowlands during an average human lifespan.
- USGS ranked Mount Rainier as a "very high threat volcano" among those volcanoes in the United States and its territories. (See fig. 21 for a national map of the location of USGS's high threat and very high threat volcanoes.) Of the 169 active volcanoes in the United States, USGS ranked 18 as very high threat volcanoes.

Hazards Description

- **Occur suddenly:** Lahars can occur with little or no warning. Most lahars large enough to flow beyond the boundaries of Mount Rainier National Park would occur during periods of volcanic unrest or eruption. For these large lahars, the estimated time between detection of a lahar on Mount Rainier and its arrival in the town of Orting, Washington, is about 40 minutes. Orting is over 10 miles from the boundary of Mount Rainier National Park and about 20 miles from the summit of Mount Rainier. Dispersed populations closer to Mount Rainier would be affected sooner.
- **Dangerous debris flow:** Lahars are fast-moving slurries of volcanic rock, mud, and water that look and behave like flowing concrete. Mount Rainier supports more than 1 cubic mile of glacial ice—as much as all other Cascade Range volcanoes combined. Thus, there is the potential to

[8]U.S. Department of the Interior, U.S. Geological Survey, Fact Sheet-034-02, *Mt. Rainier – Learning to Live with Volcanic Risk* (2002).

- **Different potential triggers:** Triggers for lahars do not have to be associated with volcanic eruptions. For example, a large flank collapse of the mountainside could also trigger a lahar at Mount Rainier. Although many flank collapses occur during eruptive periods, it is also possible for them to be triggered by earthquakes or result from the progressive weakening of rock, saturation by groundwater, and the continuing pull of gravity.

Figure 21: Location of High Threat and Very High Threat Volcanoes in the United States

Sources: GAO analysis of United States Geological Survey (USGS) data; Map Resources (map).

Appendix III: Descriptions of Communications Systems and Technologies Used by First Responders

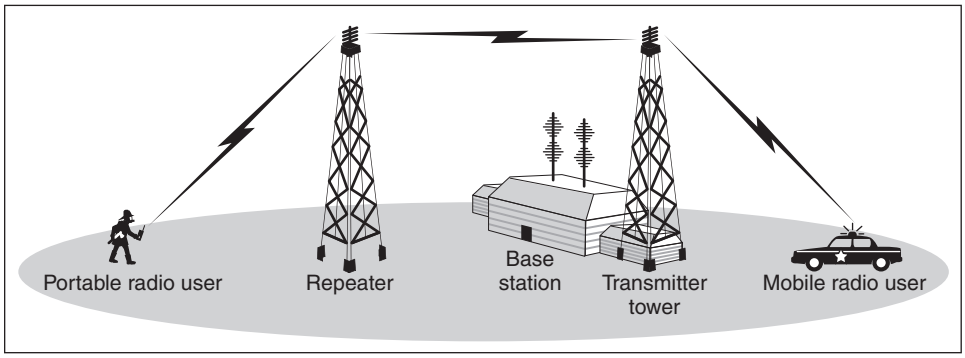
Land Mobile Radio System. Land mobile radio systems are the primary means of communications among first responders. These systems typically consist of handheld portable radios, mobile radios, base stations, and repeaters. Land mobile radio networks operate on different spectrum frequencies, such as very high frequency (VHF), ultra high frequency (UHF), 700 MHz, and 800 MHz. FCC has reported that radio handsets must operate on the same frequencies to communicate. For example, a handset operating on a specific frequency in the UHF band will not be able to directly communicate with a handset operating on a different UHF frequency or on a VHF, 700 MHz, or 800 MHz frequency. Generally, first responders must carry multiple radios to allow direct communication with radio systems operating on different frequencies.

Handheld portable radios are typically carried by first responders and tend to have a limited transmission range. Mobile radios are often located in vehicles and use the vehicle's power supply and a larger antenna, providing a greater transmission range than handheld portable radios. Base station[1] radios are located in fixed positions, such as public service access points or dispatch centers, and tend to have the most powerful transmitters. A network is required to connect the different base stations to the same communications system. Repeaters are used to increase the effective communications range of handheld portable radios, mobile radios, and base station radios by retransmitting received radio signals. Figure 22 illustrates the basic components of a land mobile radio system.[2]

[1]A base station contains the equipment for transmitting and receiving the radio signals that allow portable radios to communicate with each other.

[2]GAO-07-301, p. 11.

Figure 22: Depiction of Land Mobile Radio System



Sources: GAO and DHS.

Satellite systems. Satellite systems, such as phones, radio, and e-mail, can provide service in areas where there is no terrestrial infrastructure. The Federal Communications Commission (FCC) has reported that satellite communications, which can cover large portions of the Earth's surface, can provide an immediate backup emergency communications capability to restore emergency responder command and control communications when terrestrial infrastructure is severely damaged or destroyed.[3] Like other communications systems, orbiting satellites and their corresponding terrestrial infrastructure are not immune from threats. For example, satellites face unique space-based vulnerabilities. Typically, the terrestrial infrastructure, such as hub and gateway earth stations, is well protected, reliable, and redundant. Thus, satellite communications networks can weather terrestrial disasters if their associated earth stations survive, and can generally be restored to operation more quickly than terrestrial communications networks that rely on wireline infrastructure (see later discussion).

Cellular Systems. First responders can use systems supported by cellular technologies, including cell phones. FCC has reported that cellular technologies, which offer "anytime, anywhere" mobility, could be an important tool for responders when their primary communications systems become unavailable. For example, first responders use cellular phones for non-critical primary communications or for backup communications when primary systems fail. The existence of multiple cellular service providers with national footprints greatly increases

[3]Federal Communications Commission, *FCC Report to Congress: Vulnerability Assessment and Feasibility of Creating a Back-Up Emergency Communications System, Submitted Pursuant to Public Law No. 110-53* (Washington, D.C.: Jan. 30, 2008).

dependability and coverage even if individual commercial networks are suffering disruptions or do not necessarily meet all public safety requirements. If a cellular tower or its associated power is lost during a disaster, they could be temporarily replaced with a portable tower, backup generators, and other backup equipment.

Wireline Systems. FCC has reported that first responders depend on wireline (landline) communications for operation of critical systems. Wireline service providers design networks to minimize single points of failure that could disrupt the network. However, the strategy of no single point of failure is not applied uniformly across the network. For reasons of economy, some systems' vulnerabilities may remain. In addition, facilities connecting first responders to central facilities may use copper cable, making them vulnerable to flooding, or they may use aerial cable, which subjects them to storm and fire damage. Loss of wireline facilities was well documented during Hurricane Katrina.

Technologies to Improve Interoperability

When different jurisdictions utilize different and incompatible systems, technologies such as audio switches, crossband repeaters, and others allow different systems to interoperate. These technologies to improve interoperability are described below.

Audio Switch. An audio switch provides interoperability by sending an audio signal from one radio system to all other connected systems. An audio switch can be either stationary or mobile. One popular audio switch consists of a frame with slots, into which different hardware modules can be installed to control and interconnect different communications systems, such as VHF and UHF radios, as well as telephones. The audio switch can hold up to 12 interface modules, each capable of connecting a radio system. Audio switches are useful where multiple agencies temporarily come together to respond to an event because they are easily transportable and can be used to create temporary interoperability.

Crossband Repeater. A crossband repeater provides interoperability between systems operating on different radio frequency bands by changing frequencies between two radio systems. Crossband repeaters can connect base stations or handheld or mobile radios. The repeater is also useful for extending the communications coverage beyond the range of a single radio. Crossband repeaters can also be linked together to overcome distances or geographical features blocking communication among users utilizing one repeater.

Console-to-console patch. A console-to-console patch achieves interoperability by making an audio connection between the dispatch consoles of two different radio systems. Console-to-console patches connect consoles located at the dispatch centers where personnel receive incoming calls. These patches can connect personnel from an agency using one radio system to personnel from an agency using a different radio system. Connections between dispatch consoles can be made temporarily, as needed, through a public telephone line or permanently over a dedicated leased line or a dedicated microwave or fiber link.[4]

Software-defined radios. These radios use software to determine operating parameters such as the frequency band (such as VHF or UHF) and modulation type (such as AM or FM), and can be programmed to transmit and receive on any frequency within the limits of its hardware design. Software-defined radios will allow interoperability between agencies using different frequency bands, different operational modes (digital or analog), proprietary systems from different manufacturers, or different modulation (AM or FM). For example, a software-defined radio can be programmed to work as a conventional UHF radio but in another operating mode can function as an 800 MHz radio. Some software-defined radios could be used to identify unused frequencies and automatically make use of them, which is important in making efficient use of limited radio spectrum. The software-defined radio technology may also provide integrated voice and data over the same channel.

Voice over Internet Protocol. Voice over Internet Protocol can connect different radio systems by using an Internet Protocol network as the connecting mechanism. Voice over Internet Protocol converts analog voice signals from a radio into digital data packets that travel over an Internet Protocol network.[5] At their destination, the digital information is converted back to analog audio and can be heard on the recipient's radio. Voice over Internet Protocol enables interoperability between agencies using different frequency bands, different operational modes (digital or analog), or proprietary systems from different manufacturers. Voice over Internet Protocol holds promise as a relatively low-cost solution to communications interoperability.

[4]A leased line refers to a permanent telephone connection set up by a telecommunications provider between two geographic locations. A fiber link uses light sent over a glass or plastic fiber to carry communication signals. A microwave link uses radio beams of extremely high frequencies to send information between two fixed geographic sites.

[5]In some cases, this is the Internet; in others, it is a private data network.

Appendix IV: Stakeholder Group and Advisory Committee Descriptions

Name	Type of group	Mission	Year established
DHS Stakeholder Groups			
National Security Telecommunications Advisory Committee (NSTAC)	Stakeholder Group	To provide industry advice regarding national security and emergency preparedness and the availability and reliability of telecommunication services. Its goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help maintain a reliable, secure, and resilient national communications.	1982
SAFECOM Emergency Response Council	Stakeholder Group	To provide broad based input from the public safety community on its user needs to the SAFECOM program. A mechanism to share best practices, lessons learned, and guidance so that interested parties at all levels of government can learn from one another's experience, perspective, and expertise.	SAFECOM founded in 2001
Federal Partnership for Interoperable Communications	Stakeholder Group	To address federal wireless communications interoperability by fostering intergovernmental cooperation. Coordinating body that focuses on technical and operational matters within the federal wireless communications community, representing more than 40 federal entities.	1994
FCC Advisory Committees			
Network Reliability and Interoperability Council-VII	Advisory Committee	To partner with the FCC, the communications industry, and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices across the telecommunications industry.	2004
Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	Advisory Committee	To review the impact of Hurricane Katrina on the telecommunications and media infrastructure. The panel studied the impact of Hurricane Katrina on the telecommunications and media infrastructure, and made recommendations for improving disaster preparedness, network reliability, and communications among first responders.	2006
Joint Advisory Committee on Communications Capabilities of Emergency Medical and Public Health Care Facilities	Advisory Committee	To assess specific communications capabilities and needs of emergency medical and public health care facilities; options to accommodate growth of basic and emerging communications services; and options to improve integration of communications systems used by emergency medical and public health care facilities with existing or future emergency communications networks.	2007

Source: GAO analysis of DHS and FCC information.

Note: The FCC committees on this list no longer exist due to either termination or charter expiration. For example, the Network Reliability and Interoperability Council will be subsumed by the new Communications Security, Reliability, and Interoperability Council.

Appendix V: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 9, 2009

Mr. Dave J. Wise
Director
Physical Infrastructure Issues
Government Accountability Office
Washington D. C. 20548

Dear Mr. Wise:

Thank you for the opportunity to comment on the draft report: Emergency Communications: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts (GAO-09-604). The Department of Homeland Security (DHS) appreciates GAO's work in planning, conducting, and issuing this report.

The following represents the DHS response to the recommendations contained in the draft report.

Recommendation:

The Secretary of Homeland Security, in DHS's role as chair of the agency working group to establish the Emergency Communications Preparedness Center(ECPC), work to complete the memorandum of understanding to establish the center.

Response: Concur: Office of Emergency Communication (OEC) concurs that finalizing the ECPC through the adoption of the Memorandum of Agreement (MOA) is an important step in formalizing the ECPC's role in coordinating emergency communications across member federal agencies and facilitating implementation of the NECP. While the final Memorandum of Understanding (MOU) has not yet been approved by all member agencies, it has been signed by DHS and circulated to interagency partners for final concurrence. Throughout the Charter development process, the ECPC has been actively working on a number of key coordination and NECP implementation issues by means of staff-level working groups, including the Grants Focus Group and the Technical Assistance Focus Group. The Grants Focus Group provides a forum for Federal grant issuers to convene to share lessons learned, best practices, and information on their specific grant programs further fostering alignment among the Federal communications grant programs. The Technical Assistance Focus Group aims to identify commonalities for Technical Assistance across the federal government.

Recommendation:

The Secretary of Homeland Security and the Chair of the Federal Communications Commission (FCC) establish a forum, or other mechanism, to better collaborate on each agency's emergency communications efforts.

Concur: OEC agrees that regular, senior-level meetings between DHS, NTIA and the FCC would be beneficial. OEC notes that OEC and the FCC's Public Safety and Homeland Security Bureau have begun regular coordination meetings to identify areas for collaboration and to work jointly on common solutions as appropriate. Additional coordination will occur via the ECPC.

Recommendation:

The Secretary of Homeland Security provide guidance and technical assistance to federal agencies in developing formal emergency communications plans.

Concur: However, it should be noted that Title 18 of the Homeland Security Act focuses on assistance to "State, regional, local, and tribal governments," and provides limited authority for OEC to provide assistance to other federal agencies.

Recommendation:

The Secretary of Homeland Security and the Chair of FCC systematically track, assess, and respond to stakeholder groups' recommendations.

Concur: Though OEC concurs with this recommendation, it is important to note that OEC currently works closely with numerous stakeholder groups, including the SAFECOM Executive Committee (EC) and SAFECOM Emergency Response Council (ERC), as well as relevant critical infrastructure coordinating councils. EC/ERC meetings occur on a regular basis, and include the compilation and circulation of meeting notes and minutes. The Federal Partnership for Interoperability Coordination (FPIC) is another example of a stakeholder body that OEC has tracked and for which it has assessed recommendations. Indeed, in developing the NECP, OEC utilized these and other coordination forums to engage more than 150 stakeholders at all levels of government and the private sector. OEC also relied upon findings from the FCC's Hurricane Katrina Task Force, the FCC's Joint Advisory Committee on Public Health and the NSTAC Emergency Communications and Interoperability Task Report in developing the NECP.

Again, thank you and your staff for producing a thorough report.

Sincerely,

Jerald E. Levine
Director, Departmental GAO/OIG Liaison Office

Appendix VI: Comments from the Department of Commerce

UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

June 4, 2009

Mr. David J. Wise
Director, Physical Infrastructure Issues
Government Accountability Office
701 5th Avenue, Suite 2700
Seattle, WA 98104

Dear Mr. Wise:

Thank you for the opportunity to comment on the Government Accountability Office's (GAO) draft report entitled *Emergency Communications: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts* (GAO-09-604). Technical and editorial comments to the draft report were provided to GAO staff earlier.

As part of this engagement, GAO met with officials from two of the Department of Commerce's agencies: the National Oceanic and Atmospheric Administration (NOAA) and the National Telecommunications and Information Administration (NTIA). Among other things, NOAA provides daily weather forecasts, severe storm warnings, and climate monitoring. Its dedicated scientists provide research and use high-tech instrumentation to provide citizens, planners, emergency managers, and other decisionmakers with reliable information that may be needed during a catastrophic or other emergency event. NTIA is responsible for managing the Federal Government's use of the radio frequency spectrum. NTIA also manages the Public Safety Interoperable Communications (PSIC) grant program, which awarded $968,385,000 to fund interoperable communications projects in 56 States and Territories.

In the draft report, GAO made recommendations to improve Federal agencies' collaboration and monitoring in efforts related to emergency communications. I agree that emergency communications among first responders are of the utmost importance and that Federal agencies must be able to effectively coordinate activities to mitigate vulnerabilities. Although none of the recommendations were directed at or required specific action on the part of NOAA or NTIA, I assure you that these agencies will continue to collaborate with and support other Federal agencies in reducing vulnerabilities related to emergency communications.

Thank you again for the opportunity to share the Department's comments on this draft report. The Obama Administration is committed to strengthening this country's preparedness, response, and recovery efforts.

Sincerely,

Gary Locke

Appendix VII: Comments from the Department of the Interior

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

TAKE PRIDE IN AMERICA

JUN 3 2009

David Wise
Director, Physical Infrastructure Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C 20548

Dear Mr. Wise:

Thank you for providing the Department of the Interior the opportunity to review and comment on the draft Government Accountability Office Report entitled "EMERGENCY *COMMUNICATIONS: Vulnerabilities Remain and Limited Collaboration and Monitoring Hamper Federal Efforts*," (GAO-09-604).

We appreciate the diligent work of the team that prepared the report and the data collected. In general, we believe that this report is somewhat informative but could have been improved if it incorporated DOI or Federal interoperability collaboration efforts in regards to Emergency Response capabilities based upon the following:

- a perspective that was expanded geographically;
- interviews with DOI Emergency Management Offices;
- review of existing emergency deployment systems capabilities; and
- review of nationally recognized emergency and day-to-day interoperability efforts throughout the United States.

In addition, we suggest further interviews with the National Interagency Fire Center for a firsthand view of Emergency Communications support, capabilities and established federal practices.

The enclosure includes information regarding national policy and technical comments on the draft report.

If you have any questions, or need additional information, please contact Christopher Lewis at Christopher_Lewis@ios.doi.gov or phone, 703-648-5550.

Sincerely,

Pamela Haze

Pamela K. Haze
Deputy Assistant Secretary – Budget and Business Management

Enclosure

Appendix VIII: GAO Contact and Staff Acknowledgments

GAO Contact

David Wise (202) 512-2834 or wised@gao.gov.

Staff Acknowledgments

Other key contributors to this report were David Sausville (Assistant Director), Matt Cail (Analyst-in-Charge), Eli Albagli, Delwen Jones, John Mingus, Monica McCallum, Andrew Stavisky, Friendly Vang-Johnson, Maria Wallace, and Mindi Weisenbloom.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper