December 2014 | Vol. 80 | No. 12

APCO International

PSC

PUBLIC SAFETY COMMUNICATIONS

THE OFFICIAL MAGAZINE OF APCO INTERNATIONAL

Planning for the Future

The 2014 National Emergency Communications Plan, p. 18

Medical workers aid injured people at the finish line of the 2013 Bos ton Marathon following an explosion in Boston, Monday, April 15, 201 The 2014 NECP update takes into account many lessons learned fro large-scale emergencies, including advances in available technology. *AP Photo/Charles Krupa*

Planning for the Future

The 2014 National Emergency Communications Plan

by Ron Hewitt & Chris Essid

In 2007, the Department of Homeland Security (DHS) Office of Emergency Communications (OEC) was tasked with developing and periodically updating the National Emergency Communications Plan (NECP)—the country's first strategic plan for emergency communications.[1] OEC released the first NECP in 2008, at a time when land mobile radio (LMR) was the primary tool for maintaining mission critical voice communications. LMR remains the primary tool used by public safety for mission critical voice communications, but advances in technologies are rapidly changing the face of emergency communications. With this in mind, OEC recently spearheaded an effort to update the nation's emergency communications plan, culminating with the release of the 2014 NECP in November.[2]

The new NECP effectively balances the need to integrate existing and emerging broadband capabilities into emergency communications planning with a continued emphasis on maintaining and improving LMR systems. First responders are increasingly turning to mobile data services and applications—live video streaming, mapping and location-based services, large data file transfers, and telemetry, for example—to supplement LMR-based mission critical voice capabilities. This trend will only accelerate with the deployment of the nationwide public safety broadband network (NPSBN), which will provide broadband access exclusively for use by public safety agencies, enhancing situational awareness and information sharing capabilities.

OEC is currently providing technical assistance and support to public safety entities using commercial broadband and will continue to do so while the NPSBN is being built. Nonetheless, for some public safety agencies—especially many serving rural communities or those with limited resources to commit to new technology—maintaining and improving LMR capabilities will continue to be an emergency communications planning priority for the foreseeable future.

The Changing Communications Landscape

To capture the complexity of the emerging communications landscape, the 2014 NECP introduces an innova tive framework called the Emergency Communication Ecosystem.[3] Within this new ecosystem, OEC intends t capture existing and emerging technologies encompass ing the emergency communications environment. Th

framework conceptualizes the environment as consisting of various inter-related components and functions: incident response communications; alerts and warnings originating with the government and directed toward the public; public information exchange; and reporting and requests for assistance originating with the public and directed toward the government. This new emergency communications ecosystem brings social media and public information exchange into incident response and coordination planning for public safety.

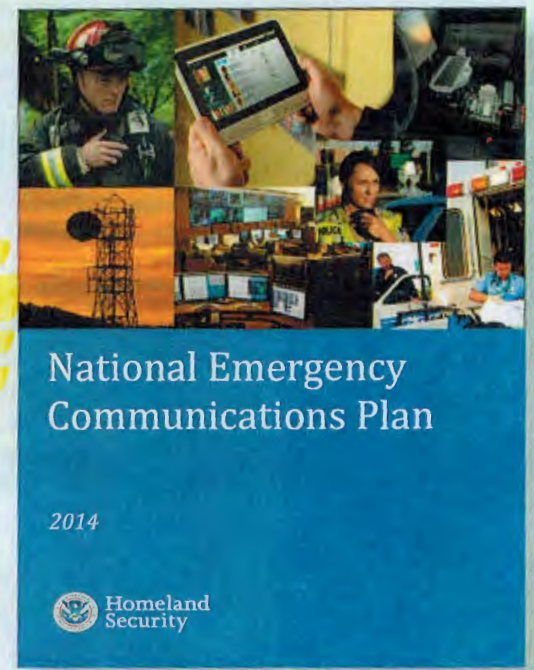
Of course, preparing for such a complicated and interconnected emergency communications landscape demands a high level of cooperation and coordination. In developing the 2014 NECP, OEC engaged more than 350 stakeholders in the emergency communications community, including representatives from all major public safety organizations, emergency management agencies, federal, state, local, tribal and territorial governments, the private sector, and others.[4] Impressive though this is, success in implementing the NECP requires sustained engagement over the long term. Navigating the new communications ecosystem presents challenges for governance and leadership, planning, training, operational coordination, and research and development.[5] These challenges can be best managed with the continued cooperation of stakeholders across the public safety spectrum and at all levels of government.

Governance & Leadership: A key challenge for governance and leadership will be planning for the deployment of the NPSBN and ensuring that emerging broadband governance structures are congruent with existing LMR governance structures. At the very least, this will require cooperation from Statewide Interoperability Coordinators and parties involved in technology procurement, information security, budgeting and emergency management.

Planning & Procedures: Traditionally, emergency communications planning has concentrated on achieving mission critical voice operability and interoperability based on LMR systems. As broadband capabilities mature, planners at agency and jurisdictional levels must develop plans, procedures and best practices for integrating broadband technology and applications into the first responder toolkit.

Training & Exercises: With appropriate training, emergency responders will learn to leverage new and emerging communications technologies to their maximum potential. Unfortunately, funding for training and exercise programs has decreased in recent years due to budgetary constraints. Consequently, public safety agencies must devise creative ways to expand and develop new training and exercise programs in the face of decreased funding.

Operational Coordination: Large-scale emergencies often present operational challenges such as power outages or communications network failures that impede communication between responding personnel and agencies. While new communications capabilities promise to make more information available to more people faster, they threaten to complicate coordinating structures and protocols. Thus, it is critical that agencies and jurisdictions work together to develop and follow a common set of operating procedures.



Research & Development: Commercial wireless broadband networks supporting presently available public safety broadband applications cannot sustain mission critical communications. As envisioned, the NPSBN will surpass commercial broadband networks in this respect. However, challenges related to cybersecurity, coverage and capacity, among others, demand further attention before the NPSBN will meet the minimum requirements for providing mission critical capabilities. Accordingly, our government, private sector and academic partners engaged in research and development must address these issues.

Emergency Response Starts at the Local Level

The 2014 NECP establishes an excellent high-level foundation for nationwide emergency communications planning for the next three to five years, but no matter what changes or challenges new technologies bring to the emergency communications ecosystem, the responsibility to respond to emergencies begins with public safety personnel at the local level. Therefore, local emergency communications planning forms the backbone of an effective national emergency communications plan. This means that local authorities must provide sound strategic guidance, effectively manage resources, develop and implement policies and operating procedures, and leverage the resources available to them to enhance emergency response capabilities.

As emergencies expand in scope, intensity or geographic impact, the responsibility to respond may extend to states. Under such circumstances, states should be prepared to provide support to local agencies whose capabilities are over-extended and, if necessary, establish procedures to call on the federal government for assistance. Key stakeholders at the state level include the Statewide Interoperability Coordinator, the State Single Point of Contact, the Statewide Interoperability Governing Body or Executive Committee, the State Emergency Management Agency Director, State Information Technology and Security Officials, and the State 9-1-1 Administrator.

In some cases, federal agencies may be called upon to support operational efforts, including support for emergency communications. However, federal involvement in emergency planning is generally limited to strategic support and guidance, such as providing funding, technical assistance and guidance, and encouraging the development and alignment of state and regional communications plans and capabilities.

OEC makes several such resources available to its partners at the state, local and regional levels. These include an extensive technical assistance program, which provides training, tools and online assistance to all U.S. states and territories.[6] This program was recently expanded to provide support to states working to integrate broadband capabilities into their statewide emergency communications plans.[7] Additionally, OEC works with SAFECOM, a stakeholder-driven emergency communications program of OEC and DHS's Office for Interoperability and Compatibility, to develop guidance for grants that provide billions of dollars annually for communications investments. The office also deploys subject matter experts at the regional level to build relationships with stakeholders, foster collaboration across state and local boundaries, and develop best practices to address emerging emergency communications challenges. Similarly, it deploys Statewide Interoperability Coordinators to develop statewide strategic plans to improve interoperability in each state.

Conclusion

The 2014 NECP boils down to three priorities: maintain and improve existing LMR systems; prepare

public safety agencies and personnel for the adoption of broadband technologies, including the NPSBN; and, enhance coordination among stakeholders.[8] In practice, this is no easy challenge—the emerging communications landscape is complex, presenting significant challenges for governance and leadership, planning, training, operational coordination, and research and development. Nonetheless, with the introduction of the Emergency Communications Ecosystem, OEC has developed an innovative and forward-thinking strategic framework to guide emergency communications planning for the next three to five years. This, along with OEC's demonstrated commitment to emergency communications stakeholders across all levels of government, suggests the nation's emergency communications leadership is up to the challenge.

RON HEWITT is the director of the U.S. Department of Homeland Security's Office of Emergency Communications.

CHRIS ESSID is the deputy director of the U.S. Department of Homeland Security's Office of Emergency Communications.

REFERENCES

1. Title XVIII of the *Homeland Security Act of 2002 in the Fiscal Year 2007 Department of Homeland Security Appropriations Act* established the Office of Emergency Communications (OEC) for the purpose of developing and implementing a strategy to achieve nationwide interoperable communications capabilities. Title 6 United States Code, § 572 granted OEC the authority to develop and periodically update the National Emergency Communications Plan.

2. US Department of Homeland Security, Office of Emergency Communications, *National Emergency Communications Plan 2014.*

3. US Department of Homeland Security, Office of Emergency Communications. *National Emergency Communications Plan 204*, pp. 10–14.

4. US Department of Homeland Security, Office of Emergency Communications, *National Emergency Communications Plan 204*, p. v.

5. See Section 3, US Department of Homeland Security, Office of Emergency Communications, *National Emergency Communications Plan 204*, pp. 15–47.

6. A comprehensive overview of the TA program is available at www.dhs.gov/office-emergency-communications-technical-assistance-program.

7. Nationwide Public Safety Broadband Network. March 2013. U.S. Department of Homeland Security, Office of Emergency Communications.

8. US Department of Homeland Security, Office of Emergency Communications, *National Emergency Communications Plan 204*, p. vi.