Interoperability Planning for Wireless Broadband

November 2011

Homeland Security

Interoperability Planning for Wireless Broadband

Office of Emergency Communications

Executive Summary

The U.S. Department of Homeland Security's Office of Emergency Communications (OEC) created this document, in coordination with the emergency response community, to help Statewide Interoperability Coordinators plan for wireless broadband use in emergency communications. Established by Congress, OEC was stood up on April 1, 2007 in response to the communications challenges witnessed during Hurricane Katrina. OEC's mission is to support and promote the ability of public safety and government officials to continue to communicate in the event of natural disasters, acts of terrorism, or other man-made disasters, and work to ensure, accelerate, and attain interoperable and operable emergency communications nationwide. In 2008, OEC published the *National Emergency Communications Plan*—the Nation's first strategic plan to address nationwide interoperable communications. Wireless broadband in emergency communications is rapidly becoming an essential component of nationwide interoperability.

This document provides an overview of broadband technology, guidance on interoperability planning for broadband, best practices from waiver jurisdictions, and regional governance considerations. Although targeted toward Statewide Interoperability Coordinators, the topics are relevant to all public safety stakeholders. This document serves as a reliable and comprehensive source of information about wireless broadband in the emergency response environment.

OEC has included two helpful appendices for emergency responders to easily remove, use, and share as part of stakeholder outreach and educational briefings on this important and emergent issue. Appendix A: Implementing Public Safety Broadband is a single-page checklist for agencies or jurisdictions implementing public safety wireless broadband. Appendix B: Wireless Broadband Fundamentals is a single-page summary of the emergency response wireless broadband topic.

Table of Contents

Executive Summary i

Introduction 1

Public Safety Broadband—Technology 101 2

Fundamentals: What is Wireless Broadband? 2

Public Safety Communications Evolution 4

Capabilities of Public Safety Broadband 4

Public Safety Technical Standards—700 MHz, LTE, and Interoperability 5

Statewide Planning 6

Roles and Responsibilities of the SWIC 6

Support from the Office of Emergency Communications 8

Highlights and Lessons Learned from Waiver Jurisdictions 10

Local Public Safety Broadband with a National Focus: Seattle, Washington 11

An Ongoing Model for Innovation and Planning: District of Columbia 12

Lessons Learned: Broadband Myths and Reality 13

Appendix A: Implementing Public Safety Wireless Broadband 15

Appendix B: Wireless Broadband Fundamentals 16

Appendix C: Organizations Working on Nationwide Public Safety Broadband 17

Appendix D: Broadband Grants and Resources 19

Appendix E: Acronyms and Common Terminology 21

Introduction

Wireless broadband for use in public safety (hereinafter referred to as "wireless broadband") is becoming more prominent within the emergency response community. Many readers will be familiar with commercial wireless broadband services, such as the networks used to support smartphones and mobile Internet; some may already use wireless broadband in emergency response. As with any emerging technology in a mobile environment, speeds and capabilities vary widely between networks and devices.

In the context of emergency response, broadband presents several attractive capabilities—many of which are already in use on commercial networks. Firefighters using wireless broadband can download blueprints for a burning building while in the field, a police officer can receive surveillance video feeds while on-scene, and emergency medical services (EMS) personnel are able to remotely access or transmit medical information. Depending on the network's speed, some on-scene personnel can transmit live video feeds or pictures to their incident commander, enhancing situational awareness. Each of these capabilities significantly improves emergency communications and levels of response.

It is important to note that as it stands today, wireless broadband will supplement—not replace—land mobile radio (LMR) for voice communications. The cost and time involved with the creation of a nationwide public safety wireless broadband network are substantial, and emergency communications stakeholders should assume LMR will remain the primary voice communications system for years.

Statewide Interoperability Coordinators (SWICs) should be involved in broadband efforts for public safety to ensure emerging technologies are incorporated into strategic plans. In addition, existing governance structures should be utilized to ensure planned technologies meet the needs of emergency responders, complement existing voice communications, and will be interoperable. By getting involved, SWICs will gain familiarity with networks that they will ultimately be responsible for coordinating, as wireless broadband is sure to become an essential part of State and local emergency communications.

> "We're going to invest in research and development of emerging technologies and applications....and deploy a new nationwide, interoperable wireless network for first responders—making sure they've got the funding and the frequencies that they were promised and that they need to keep us safe."
>
> **President Barack Obama**
> **National Wireless Initiative Remarks**
> **Marquette, Michigan**
> **February 10, 2011**

Public Safety Broadband—Technology 101

This section explains the fundamentals of wireless broadband in order to educate and inform SWICs and the emergency response community. The purpose is not to make the reader an expert in public safety broadband technologies; rather, the guidance document provides context for readers to begin planning for public safety broadband in their States, regions, and localities.

This section will: (1) explain the fundamentals of broadband; (2) introduce the Public Safety Communications Evolution vision and graphic; (3) identify capabilities associated with public safety broadband; and (4) briefly explain technical standards as they relate to public safety broadband planning.

Fundamentals: What is Wireless Broadband?

Wireless broadband is increasingly being embraced by the public, to support new services and applications on devices such as laptops, smartphones, and digital tablets. The architecture (infrastructure) over which these devices communicate is well proven and more than 300 million wireless broadband subscribers worldwide.[1] Simply put, broadband refers to advanced communications systems capable of providing high-speed transmission of data, voice, and video over the Internet and other networks.

Wireless Broadband Terminology

The emergency response community has grown accustomed to, and reliant upon, LMR systems. Responders know that dispatch centers, mobile radios, and portable radios can all communicate with each other using spectrum that has been allocated to public safety by the Federal Communications Commission (FCC).

As broadband becomes a part of the public safety conversation, responders must learn a new series of terms and phrases. Figure 1 explains wireless technology generation terms. While each represents the evolution of broadband technology, this document will focus on Long Term Evolution (LTE), as it has been endorsed by public safety and adopted by the FCC as the technology platform for use by public safety in the 700 MHz band.

Figure 1 Wireless Technology Generations

The wireless industry notes the progression of wireless technology in terms of "**generations**."

- First-generation wireless includes voice-only communications devices such as the **analog** cellular phone.
- Second-generation wireless introduced **digital** wireless and includes personal communications service devices that offer voice and text.
- Third-generation encompasses **smartphones** and other **advanced devices** that provide voice, text, and Internet capabilities. These devices can run a multitude of applications, in many cases simultaneously.
- Fourth-generation wireless and LTE are being designed to provide **higher speeds and more advanced applications** such as streaming video.

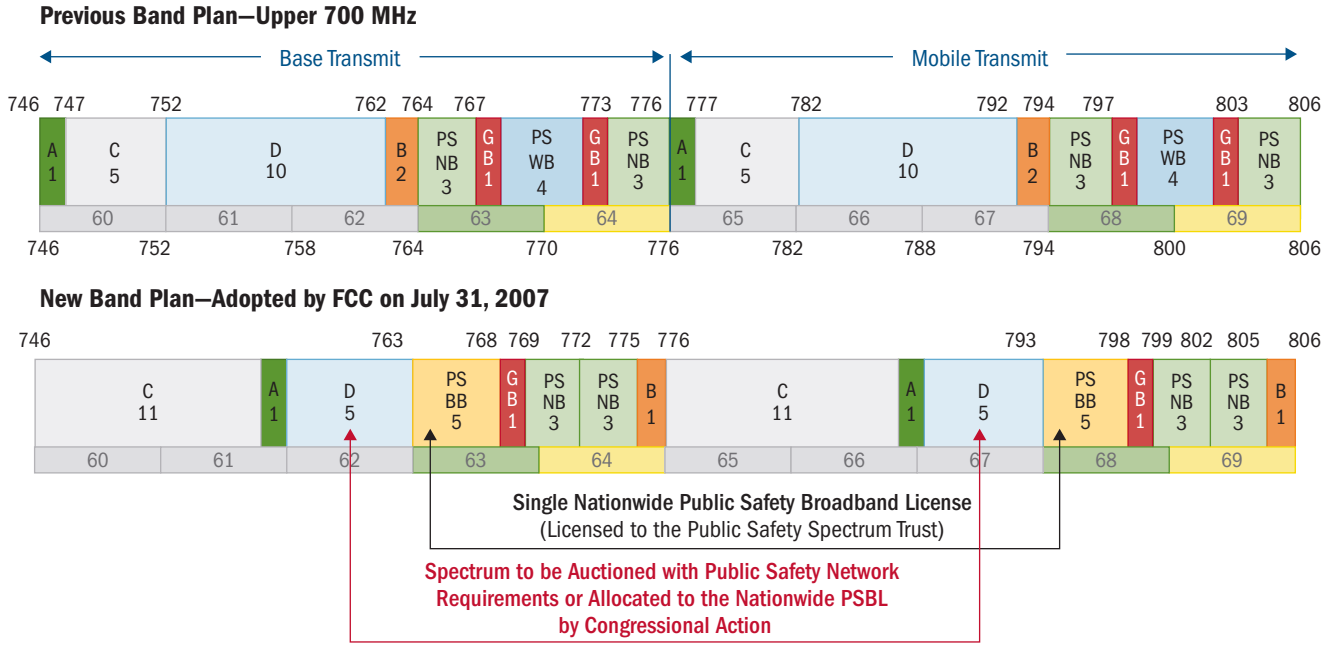
1 According to CTIA-The Wireless Association *http://www.ctia.org/advocacy/research/index.cfm/AID/10316*.

Wireless Broadband for Public Safety

In July 2007, the FCC revised its 700 MHz band plan and service rules to promote the creation of an interoperable nationwide public safety broadband network. As detailed in Figure 2, a portion of the band was designated for broadband public safety communications and existing narrowband public safety allocations were consolidated. Finally, in 2007, the FCC established a single nationwide license—the Public Safety Broadband License (PSBL)—for the 769-775/799-805 MHz spectrum, and granted that license to the *Public Safety Spectrum Trust (PSST)*.[2]

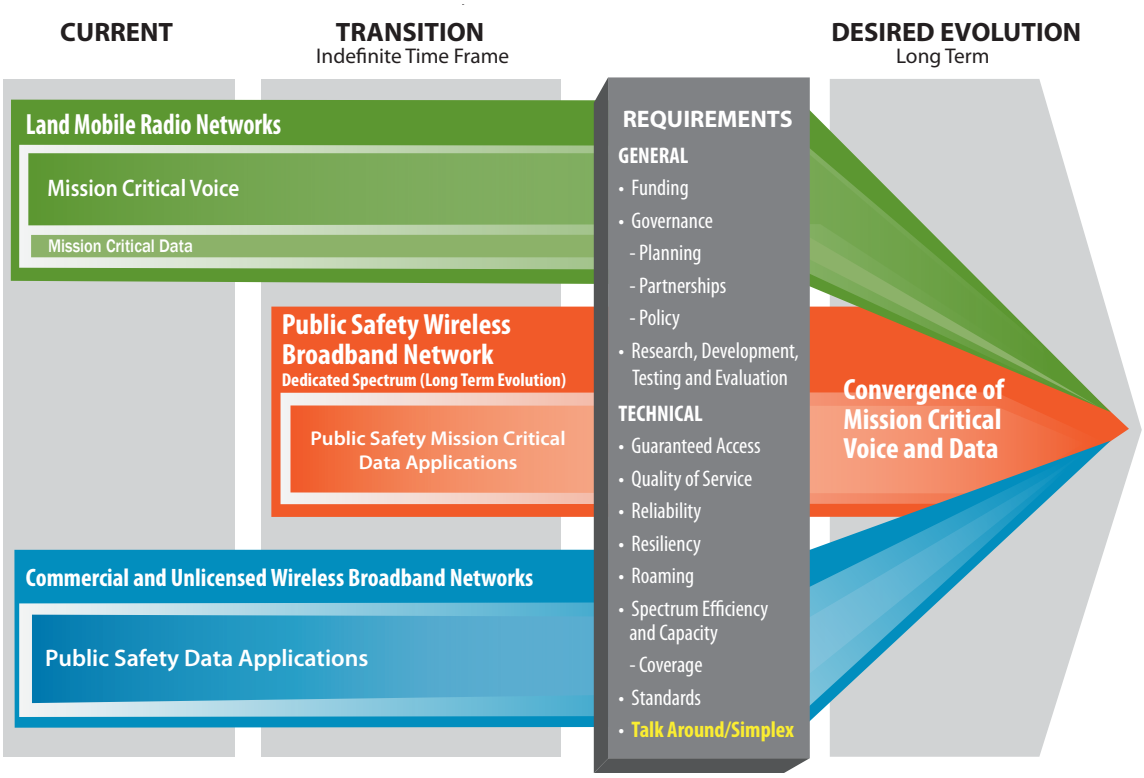
> "LTE doesn't deliver national interoperability on its own. It delivers an interoperability framework, but that's not real interoperability. Real interoperability allows individuals to share useful information. If configured properly, LTE will allow IP packets to be exchanged, but if a user's applications can't decipher the packet contents to deliver useful text, images, video, audio, resource availability, telemetry, or other content, then it hasn't achieved interoperability. Public safety needs to develop standards for information flow for real interoperability to occur."
>
> **NPSTC AFST Chair Joe Ross**
> **"The Truth About LTE" MissionCritical Communications Magazine, November/December 2010. Reprinted with permission from Joe Ross and MissionCritical Communications Magazine**

Figure 2 700 MHz Spectrum



2 Implementing a Nationwide, Broadband Interoperable Public Safety Network in the 700 MHz Band, FCC Docket 06-229, dated November 19, 2007—refer *http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-199A1.pdf*

Figure 3 Public Safety Communications Evolution



Public Safety Communications Evolution

The public safety community's vision of the *evolution of public safety communications* as it transitions from today's technology to the desired long-term state of convergence is depicted in Figure 3, which outlines a conceptual framework for building wireless broadband communications while maintaining LMR networks to support mission critical voice communications. In the current state of communications, LMR networks, commercial broadband networks, and a nationwide public safety wireless broadband network are evolving in parallel. As communications evolve, public safety will continue to use the reliable mission critical voice communications offered by traditional LMR systems; at the same time, agencies will begin to implement emerging wireless broadband services and applications. During the transition period, public safety will begin building out a dedicated public safety wireless broadband network and public safety organizations will begin to transition from commercial broadband services to the public safety dedicated network. If and when the technical and non-technical requirements can be met and are proven to achieve mission critical voice capability, it is desired that over time agencies will migrate entirely to this broadband technology. Since wireless broadband technology does not yet currently support a mission critical voice capability (talk around/simplex/direct mode), there will be a significant period of time where both wireless broadband and traditional LMR are necessary.

Capabilities of Public Safety Broadband

As the Nation increasingly uses broadband technologies, it is important to consider how emergency responders will use a nationwide public safety wireless broadband network. What types of applications does the emergency response community need or want? How will these applications ensure interoperability? How will emergency preparedness and response capabilities be enhanced through the use of broadband and these applications?

In 2010, the National Public Safety Telecommunications Council (NPSTC) conducted a nationwide assessment of issues involving spectrum and future operations. The assessment, done on behalf of NPSTC's *Assessment of Future Spectrum and Technology (AFST) Working Group*, included a Web-based survey and a series of half-day focus group sessions in Southern California; Houston, Texas; Orlando, Florida; and Washington, DC. During the sessions, public safety representatives provided operational feedback on a specific emergency event in their jurisdiction. AFST collected a large amount of information in each session, including specific operational needs at the scene of an emergency, as well as a list of data and video applications that are needed

to support the emergency response community. A full explanation of the assessment findings is expected to be released in late 2011.

NPSTC provided preliminary findings to OEC to help prepare this document and maximize the value of information to stakeholders. Information shared included a list of applications that public safety agencies identified as critical to emergency communications. The applications listed were surprisingly similar, regardless of the geography of that region (e.g., urban, rural, desert, mountains) or the emergency events that were selected (e.g., hurricanes, toxic gas leaks, wild land fires, chemical plants explosions). All agencies reported that access to geographic information system (GIS) files is critical, as well as the need for real-time video feeds from the incident scene to the incident commander. Although the results are still being compiled by NPSTC, a preliminary list of applications identified by emergency responders includes:

- Automatic Vehicle Location
- Incident Command White Board
- Aerial Video
- Vehicle-Mounted Video
- Helmet Cameras
- Third-Party Camera Resources
- Mobile Data Computers
- Patient, Evacuee, and Deceased Tracking
- Internet Connection
- Bio Telemetry
- Third-Party Sensors

Wireless broadband applications have the potential to increase emergency preparedness and response capabilities, thereby transforming the way emergency responders perform their jobs. To ensure responders' needs are met, public safety must insist that broadband networks deliver highly reliable public safety-grade services and applications.

Public safety broadband networks must accomplish a number of objectives. Specifically, the network must: (1) deliver broadband communications that meet the appropriate public safety grade operational requirements for reliability and security; (2) secure the trust of public safety agencies that will migrate traffic to this new network; (3) enable seamless communications between public safety agencies and jurisdictions; (4) provide a platform for a wide range of affordable equipment and applications; and (5) leverage, to the largest extent possible, commercial platforms and technologies that can evolve to take advantage of innovation on a cost-effective basis.

Public Safety Technical Standards—700 MHz, LTE, and Interoperability

LTE first emerged as a de facto technological standard in the commercial sector. The public safety community noted that many major telecommunications companies had adopted LTE or announced plans to do so, and a public safety consensus emerged in support of adopting LTE as the air interface for the public safety broadband network. The FCC subsequently adopted LTE as the technology standard for the nationwide public safety broadband network, an action supported by the PSST and public safety professionals from the *Association of Public-Safety Communications Officials-International (APCO)*, *NPSTC*, the *National Emergency Number Association (NENA)*, and other public safety stakeholders.

In May 2010, the FCC granted conditional waivers to 21 jurisdictions to begin building 700MHz broadband systems that will become part of the nationwide network. On September 2, 2010, the FCC approved broadband spectrum leases between the PSST, which holds the nationwide PSBL, and 20 of these waiver jurisdictions. The State of Texas waiver was granted on May 12, 2011.

On December 10, 2010, on the recommendation of the *Emergency Response Interoperability Center (ERIC)*, the FCC approved an initial set of technical requirements for those public safety jurisdictions that were granted conditional waivers. The FCC allowed the waiver jurisdictions to proceed with deployment of their 700 MHz wireless broadband networks upon certification of their compliance with the technical requirements. The initial set of *technical interoperability requirements* creates a baseline technical interoperability framework for actual deployment of public safety broadband networks. The FCC went on to specify performance, coverage, and other requirements necessary to ensure the networks achieve a baseline of communications operability. ERIC is leading FCC efforts, working in coordination with the Public Safety Broadband Licensee (currently the *PSST*); public safety representatives; the waiver jurisdictions; and the broader emergency response community.

Statewide Planning

There is no better opportunity for SWICs to exercise leadership than by helping States prepare and plan for a nationwide public safety broadband network. The objective is clear: establish a fully interoperable, nationwide public safety wireless broadband network to ensure the network can get the right information to the right people at the right time. This will allow public safety at all levels of government to better manage day-to-day activities and non-routine incidents. States are the natural building blocks of a nationwide network, and SWICs, as part of the statewide structure, can act as a central coordination point for information, nationwide strategies, education of their public safety agencies, and coordination of interstate and intrastate broadband build-outs.

Roles and Responsibilities of the SWIC

It is important that SWICs be aware of the broadband efforts currently underway; it is especially important for SWICs to recognize how Federal agencies are working together with stakeholders and industry to address broadband issues. There is no doubt as public safety stakeholders continue to actively utilize broadband, questions about the viability and reliability of the nationwide public safety wireless broadband network and the use of both 700 MHz and LTE technology will continue. It is essential SWICs be able to speak intelligently about these topics and provide answers to stakeholders and elected officials.

To help wireless broadband adoption in their State, SWICs should:

- Identify wireless broadband stakeholders throughout the State.
- Engage wireless broadband stakeholders with current interoperability governance structures.
- Start planning for wireless broadband use in their State.
- Facilitate the adoption of interoperable wireless broadband in their State.

Advice from Stakeholders

OEC interviewed a group of public safety stakeholders and technology experts. They noted the following about a nationwide wireless broadband network:

It will take time, money, leadership, coordination, collaboration, and communication to accomplish the necessary standards for a nationwide public safety broadband network.

It will take active participation at all levels and by all Federal, State, local, and tribal agencies, elected officials, SWICs, public safety professional organizations and associations, emergency responders, and industry.

Identifying Stakeholders

SWICs must first identify the appropriate stakeholders throughout the State. Broadband expands the list of traditional public safety stakeholders to include more non-traditional stakeholders. The list of potential stakeholders includes, but is not limited to, the following:

- Chief Information/Chief Technology Officer
- State broadband task force
- Statewide Interoperability Governing Body (SIGB)
- Regional Interoperability Committees
- Recipients of waivers from the FCC, including those receiving broadband grants through the Broadband Technology Opportunities Program (BTOP)
- Urban Areas Security Initiative (UASI) representatives
- State agencies
- Federal agencies, especially Federal emergency responders
- Commercial broadband vendors
- SWICs from bordering States

Keep in mind broadband networks will cross State and eventually international borders. States will need to prepare and plan for broadband together to achieve nationwide interoperability. Exchanging lessons learned and pooling resources will enhance the capacity and interoperability of wireless broadband networks.

Engaging Stakeholders

Once the SWIC has identified the relevant broadband stakeholders, the SWIC should begin to engage them in statewide interoperability efforts. SWICs should participate in meetings for broadband projects in their State, and invite points of contact for broadband projects to present at SIGB and regional interoperability committee meetings. It is recommended to incorporate broadband into preexisting governance structures rather than establish separate broadband governance groups. Integrating wireless broadband governance into existing interoperability governance structures paves the way for adding other stakeholders to the overall interoperability conversation. Outreach efforts should also take into account stakeholders' level of familiarity with broadband technology. Some public safety professionals may not see the need for wireless broadband, whereas those with more experience using broadband technology may misplace trust in its capacity and reliability as a replacement for LMR voice communications. SWICs should consider varying levels of outreach to educate public safety and other stakeholders on the current capabilities of broadband technology.

Considerations for Public Safety Broadband Planning

To better understand how to plan for public safety broadband, OEC engaged public safety stakeholders and subject matter experts actively working on public safety broadband (e.g., SWICs, representatives from the FCC waiver jurisdictions, industry professionals, and other emergency communications stakeholders). OEC used these discussions to gather input, share perspectives, and identify important considerations for implementing public safety broadband.

These discussions generated "Things to Consider" for SWICs and others in leadership positions to reference as they plan for and implement wireless broadband. This list is meant to encourage ideas and dialogue among the public safety community and States as they further investigate broadband.

The creation and implementation of a nationwide public safety broadband network will require significant collaboration, coordination, and partnerships. The next 3 to 5 years will provide incremental documentation of lessons learned and best practice examples, like those cited in this guidance document, to help others as they evaluate and assess how broadband technology will impact their States.

Things to Consider:

- Know the risk factors: recurring costs to manage, maintain, and refresh a network are considerable.
- Educate and inform your stakeholders about what is underway.
- Define your needs early on: know what you want to access or share, plus when and for what purposes.
- Make sure governance structures are in place in advance: leverage the SIGB and regional interoperability committees.
- Take a leadership role: bring a wide variety of public safety stakeholders, such as information technology partners, neighboring States, and Federal agencies, into the discussions early on.

The overall policy and regulatory framework has not yet been finalized for wireless broadband, so SWICs must account for that uncertainty and ultimately ensure their efforts align with the final framework, as well as State and regional goals. OEC resources currently available on statewide and regional interoperable communications planning include:

- *Establishing Governance to Achieve Statewide Communications Interoperability: A Guide for Statewide Communication Interoperability Plan (SCIP) Implementation*
- *Regional Intrastate Governance Guide*
- *Regional Interoperability Communications Plan*

SWICs can facilitate the adoption and use of broadband in several ways:

Wireless Broadband and the SCIP: Wireless broadband capabilities and interoperability considerations should be addressed in strategic planning documents such as the SCIP as early as possible. Broadband governance will add another dimension to SCIPs and statewide planning, but should not be isolated from existing networks and governance bodies.

Advice to SWICs:

"There's still a lot of things SWICs can do in relation to promoting broadband, conducting outreach, reaching out to constituents, building relationships with their State's stakeholders, and letting people know this is something that will be important both at the State level and nationally."

Michael Crews
California Statewide Interoperability Coordinator
California Department of Emergency Management

Education and Outreach: As with most existing public safety networks, many broadband networks will ultimately be financed by taxpayer dollars allocated by elected officials. Taxpayers and elected officials who have a basic knowledge of wireless broadband and the benefits it offers emergency response are much more likely to support broadband. The SWIC can work to promote a better understanding of the need for broadband in public safety.

Grant Funding: Funding will be critical for emerging broadband networks. SWICs should use existing relationships, especially with the State Administrative Agency (SAA) to identify opportunities for broadband-eligible grants with their stakeholders. Appendix D provides a list of grant programs that fund broadband activities.

Connections: SWICs can assist broadband stakeholders by connecting them with valuable contacts or resources to support their project. SWICs tend to have wider visibility of national and statewide public safety operations than regional or local stakeholders. Therefore, SWICs may be able to identify important stakeholders that the local broadband projects may not have considered initially, such as neighboring States, secondary responders such as transportation departments, and other public service agencies. To ensure that wireless broadband projects are interoperable from the beginning, SWICs should encourage consideration of border issues and public-private partnerships as well.

Life Cycle Planning: The SWIC can identify guidance documents and other resources to help emergency responders and elected officials anticipate ongoing costs of maintaining a wireless broadband network. A list of helpful resources is included in Appendix D.

Legal Counsel: As broadband is integrated into emergency communications, public-private partnerships, procurement activity, Memoranda of Understanding, or Joint Powers Agreements will be necessary. The SWIC should advise broadband stakeholders to involve legal counsel at their project's onset to establish clear lines of fiscal and operational responsibility.

Perspective: SWICs can ensure regional or local broadband systems comply with FCC standards and stakeholders are not duplicating work done elsewhere. SWICs also have the opportunity to not only collect best practices from within their State and share them with stakeholders, but also learn from other States via the National Council of Statewide Interoperability Coordinators (NCSWIC). Additionally, the SWIC may have knowledge of the relationships between agencies that impact wireless broadband nationally or in their State, and can ensure local stakeholders are cognizant of those relationships

Support from the Office of Emergency Communications

OEC supports the deployment of the nationwide public safety broadband network by helping to set the broad policy framework and soliciting and incorporating the views and requirements of the public safety community in network broadband planning and implementation efforts. OEC continues to work with other DHS components, the FCC, and the Departments of Commerce and Justice. OEC is also:

- Updating the NECP to include operational and technological wireless broadband information; these updates will support future public safety needs.
- Supporting States and regions on broadband planning and implementation through technical assistance (TA).
- Ensuring States are ready for broadband deployment by encouraging the introduction of broadband planning into SCIPs.
- Educating and informing emergency responders about wireless broadband.
- Working with SAFECOM; the NCSWIC; and representatives of State, regional, local, and tribal entities to ensure that the communications and interoperability needs of the public safety community are met.

To ensure the successful interoperability planning and coordination established over the past 10 years is not undone with the introduction of next-generation technologies, public safety will require more than just the technology itself. It will require leadership from the top down and bottom up, thoughtful planning, coordination, and continuing dialogue.

OEC Technical Assistance Offering: Public Safety Broadband Transition Planning

An important part of planning for a public safety broadband network involves assessing the current state of interoperable emergency communications capabilities, and establishing a vision, set of goals, and priorities for the effort. To assist with this effort, OEC has created a TA service offering for emergency responders planning for a wireless broadband network. The "Public Safety Broadband Transition Planning" template helps stakeholders identify their current and potential types of data, sources, and uses of mission-relevant information, with the goal of collecting all data necessary for a community to plan for the adoption of wireless broadband technology. This information is then captured in the "Public Safety Wireless Data" report and can assist emergency responders in clarifying requirements for wireless broadband.

Highlights and Lessons Learned from Waiver Jurisdictions

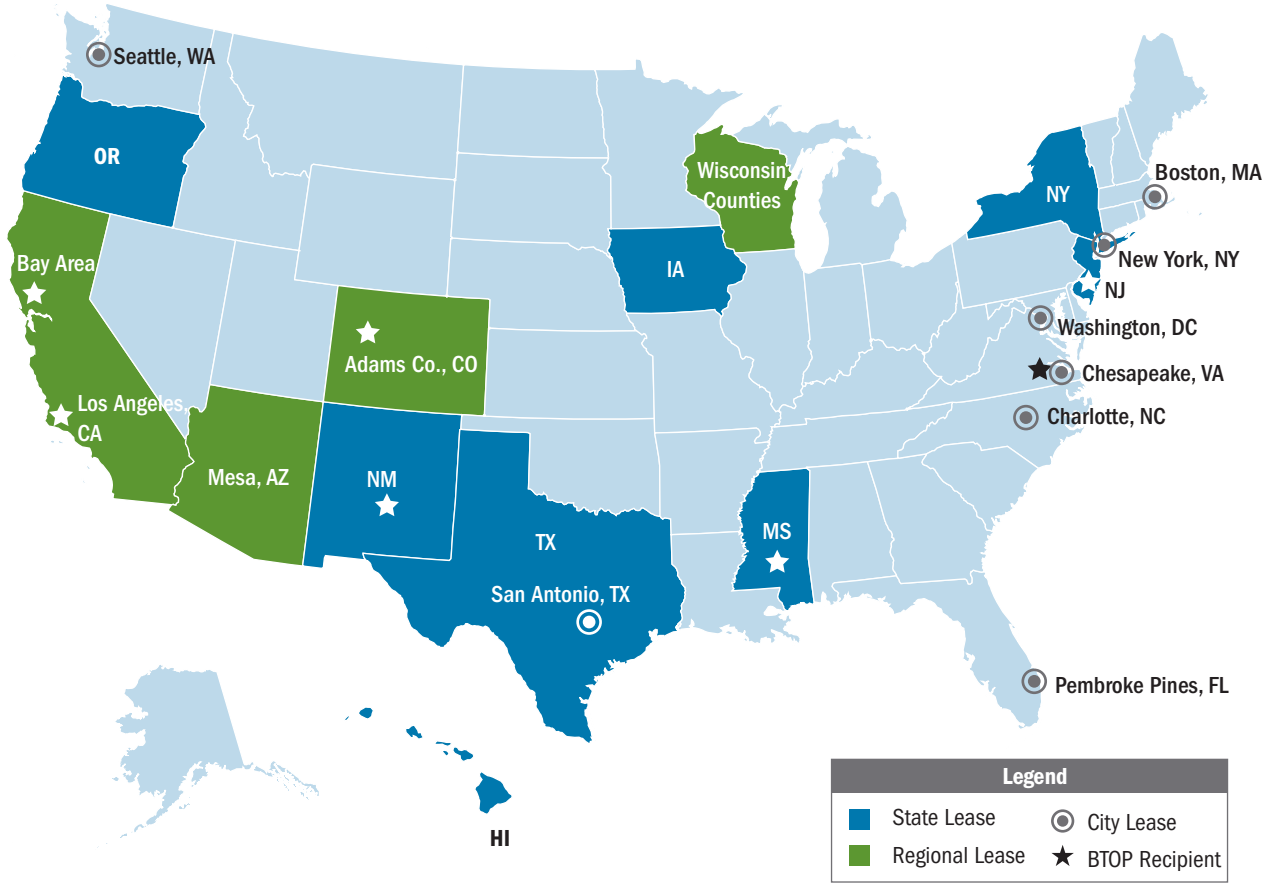
Regardless of the technology, reviewing best practices and examples of shared knowledge and experiences in wireless broadband is a good starting point for public safety stakeholders who wish to adopt a similar model. Collaboration is critical, but in today's environment, successful emergency response requires the ability to effectively share data and information across multiple jurisdictional boundaries in a secure and efficient manner. To be effective, wireless broadband initiatives must combine next-generation technology and individuals committed to working together. States and regions must be willing to forge new relationships and find new and innovative ways to better collaborate and explore creative methods and protocols for information-sharing. While a single, fully integrated nationwide system able to provide information to every public safety agency in the Nation is ideal, progress has been made through bringing regional partners together in voluntary collaboration.

Waiver Jurisdictions

In 2010, the FCC released an Order granting conditional waivers to 21 State and local public safety petitioners to begin building 700MHz broadband systems that will become part of the nationwide network. This waiver provides the jurisdictions with access to the 10MHz of broadband spectrum currently licensed to the PSST through a lease with the PSST. As part of the FCC conditions, these waiver jurisdictions–often referred to as early adopters–will have to effectively demonstrate deployment plans and network compliance that meet guidelines adopted by the FCC. In 2011, the FCC granted an additional waiver to the State of Texas.

The 21 entities complying with these waiver requirements, who now have negotiated leases with the PSST, are illustrated in Figure 4. Seven of the jurisdictions (highlighted with a star on map) have received grant funding of approximately $380

Figure 4 Waiver Recipients



million through the National Telecommunications and Information Administration (NTIA) Broadband Technology Opportunity Program (BTOP). Some jurisdictions are accessing other grant programs or State and local funding for planning and implementation efforts.

700 MHz Network Testing and Deployment

These 21 waiver jurisdictions will have the responsibility to break new ground on behalf of the emergency response community. They will serve as the proving ground for public safety broadband and, together with the Federal agencies supporting this effort, will be responsible for bringing stakeholders together, breaking down old process silos, and ensuring the nationwide public safety broadband network is both interoperable and meets the requirements of public safety and the Nation. Ultimately, the waiver jurisdictions are responsible for deploying their local facilities in such a way that they can eventually be integrated into a truly interoperable nationwide network. The representatives from the waiver jurisdictions serve as members of a PSST Operator Advisory Committee (OAC). The purpose of the OAC is to facilitate coordination and communication between the PSST and the waiver entities.

The Public Safety Communications Research (PSCR) program, which is part of the National Institute of Standards and Technology (NIST) and co-managed by NIST and NTIA of the Department of Commerce has built a *700 MHz Public Safety Broadband Demonstration Network* to test hardware and applications in advance of deploying the systems in a multi-vendor, vendor agnostic, host environment. One of the mandates from the FCC as part of the PSBL is all manufacturers' equipment must be tested and certified by PSCR prior to being deployed. Vendor-agnostic test results will be available to the emergency response community and the waiver jurisdictions. The PSCR website serves as an up-to-date reference for those interested in tracking the testing and evaluation process. Waiver jurisdictions are working closely with PSCR to test and evaluate new technology.

Local Public Safety Broadband with a National Focus: Seattle, Washington

Like its colleagues in waiver jurisdictions across the Nation, the City of Seattle is making great strides to ensure public safety broadband will meet the needs of its own 15,000-member public safety community within King County, Washington. Seattle is also focused on the importance of looking at its facilities and technology as an integral part of a nationwide public safety broadband network that extends beyond the needs of its local agencies and regions. Seattle believes expanding the user base on its network to include additional secondary responders will be the key to building and sustaining the nationwide public safety broadband network. For Seattle, these non-traditional public safety users include electrical and water utility workers, transportation services with responsibility for emergency evacuations during disasters, hospitals, and government offices, including the education system.

King County, Washington covers 2,314 square miles and ranks as the 14th most populous county in the Nation with 1.9 million people. The Seattle area is one of the country's leading high-tech regions, home to Microsoft and a host of other high-tech and Fortune 500 companies. With highly advanced and interoperable LMR systems the City of Seattle, King, Snohomish, and Pierce Counties have a long history of collaborating in emergency communications. Under the stewardship of Seattle's Chief Technology Officer (CTO) Bill Schrier and an Information Technology (IT) department that is a focal point for regional IT and telecommunications efforts, Seattle is now looking to the next generation of wireless communications: a LTE wireless broadband network.

National Vision

In a phased planning strategy, Seattle will focus first on its own wireless broadband efforts, then expand to the Four-County Central Puget Sound Region, then across the State, and finally, into nationwide interoperability.

> "The 700 MHz broadband network across the Nation is so important. We are not only looking at the local and regional point of view—we have options for our region now, but we want to be part of the national effort!"
>
> **Bill Schrier**
> **Chief Technology Officer**
> **City of Seattle**

To ensure its focus remains centered on nationwide public safety broadband objectives, CTO Schrier and Seattle Director of Major Projects Stan Wu are both actively engaged on committees discussing broadband from a national perspective, including ERIC's *Public Safety Advisory Committee (PSAC)* and *Technical Advisory Committee (TAC)*. In addition, Schrier is the current Chair of PSST's Operator Advisory Committee and President of the *Metropolitan Information Exchange*, which brings

Broadband Planning With a Local and National Focus

The City of Seattle continues in its wireless broadband planning efforts and participates in a regional group which is actively preparing and coordinating LMR and LTE roadmaps for the region. A preliminary design report for its own broadband network recommended 34 LTE radio access network sites; however, it expects the list of sites to change when the Request for Proposal (RFP) process is complete, vendor site surveys are conducted, and detailed site engineering work occurs. The release of the RFP will follow the finalization of its preferred strategy for implementation and funding currently under development.

Aware that their local efforts will have implications on a nationwide network and what happens nationally will impact their efforts, Seattle staff remain heavily engaged at the national level, participating and serving in leadership roles on committees and initiatives whenever wireless broadband is being discussed.

together Chief Information Officers (CIOs) of major cities to share knowledge and best practices regarding how operability and interoperability needs may be met. Participation in public safety broadband on a national level only serves to enhance their local efforts.

State and Local Vision

Even as Seattle and the State of Washington play a key role in broader collaboration on the development of a nationwide public safety broadband network, their leadership is ensuring that local planning efforts are solid. Seattle has looked to, and relied upon, the leadership of former SWIC Alan Komenski to ensure the work in Seattle extends beyond its borders and across the State of Washington. Additionally, Seattle has worked tirelessly to ensure the wireless broadband needs of its citizens and the emergency response communities are met, and the right outreach and education continues to keep broadband in the forefront of priorities for elected officials and governing bodies.

Komenski acknowledged it will take time for this type of technology to evolve and become available. The challenge is keeping others cognizant of that timeline and the fact that existing voice LMR systems will have to be sustained and maybe even replaced before broadband can meet all of public safety's mission critical needs. Komenski noted that simply because voice LMR will be around for years to come, it does not mean regions should not move quickly on planning efforts for broadband.

Washington State touts the importance of its long-standing relationships that have built trust throughout the emergency response community. Through these relationships, everyone knows each individual or group has an opportunity to have a role in all interoperable communications-related decisions. The work to build public safety broadband for its constituents and to play a role in the larger effort to build a nationwide public safety broadband network continues for Seattle and regions throughout the State. Komenski noted that "a lot of different partnerships are needed to create a successful broadband network." This is a "viewpoint that extends beyond its borders to the benefits of nationwide public safety broadband."

An Ongoing Model for Innovation and Planning: District of Columbia

The District of Columbia (DC) is no novice when it comes to deploying innovative and leading-edge technologies. For almost a decade, it has made wireless voice and data applications a priority under the leadership of the DC Office of the Chief Technology Officer (OCTO). Since 2004, DC has carried out a number of public safety wireless broadband evaluation and demonstration projects, including one that was selected by the NTIA as a model demonstration project to test the operations and cost effectiveness of network sharing among Federal, State, and local departments.

The pilot project, *Wireless Accelerated Response Network (WARN)*, was a broadband public safety wireless network providing coverage throughout the city. WARN became operational in June 2005 under an experimental 700 MHz license and effectively demonstrated public safety mobile broadband applications for Federal, State, and local users. Following the WARN project, DC and the other National Capital Region (NCR) jurisdictions undertook an effort to deploy a 3G network throughout the NCR, using UASI grant funds. The Regional Wireless Broadband Network (RWBN) was designed to cover the NCR, but regulatory changes in 2007 led regional executives to defund the project before first phase deployment was

A Regional Collaboration in the Mid-Atlantic

Led by SWICs from the five States (Delaware, Maryland, Pennsylvania, Virginia, West Virginia) and the District of Columbia that make up FEMA Region III, the advance planning work is underway for a public safety wireless broadband network in the region. The project is federally funded through the Regional Catastrophic Preparedness Grant Program.

Under this project, these five States and the District are proceeding with the governance, network planning, and procurement work necessary to prepare for deployment of a region-wide section of the nationwide public safety broadband network. The project aims to obtain top-level executive support, establish a multi-State governance mechanism, and aggregate the States' buying power into a single procurement approach to drive down both capital and operational costs. When each State is ready to build, this project will help make sure the pieces are already in place to maximize interoperability and minimize expense.

complete. DC gained three more years of 700 MHz public safety broadband experience from the RWBN and decommissioned the network in 2010.

The District is now working with the surrounding States (Delaware, Maryland, Pennsylvania, Virginia, and West Virginia) to plan and design a regional public safety broadband network using LTE technology. This regional effort would set the stage for deployment of a substantial portion of the nationwide public safety broadband network. Interoperability is a key concern for DC and OCTO. "Interoperability in the Nation's capital is an imperative," said Kenneth Boley, the former Director of Intergovernmental Initiatives. "The interoperability requirements here are elevated–DC and Federal first responders work closely together here every day, including public safety personnel from jurisdictions in Virginia and Maryland. The cooperative planning work to achieve interoperability here is enormous." "To accomplish that planning work, engaging stakeholders at the highest levels is critical. It helps that public safety broadband is now elevated to a national policy issue, but it takes time. Technology is key, but governance and planning are every bit as important," said Boley.

Lessons Learned: Broadband Myths and Reality

Stakeholders engaged by OEC in this effort said it was important that solid and reliable information be provided to dispel some of the myths, misunderstandings, and misperceptions of public safety broadband. These myths and reality statements provided below are intended to inspire thought around the issue of public safety broadband and to help SWICs, planners, and other leaders beginning this process better understand the complexities of this issue and how to help ensure that misinformation is not perpetuated.

The myths and realities outlined on the following page are just a sample of those that currently exist, and those that may exist in the future concerning public safety broadband. In particular, one theme resonates clearly: Planning, design, and specifications/requirements are essential components to successful deployment of a nationwide public safety broadband network. It will be important to ask the right questions, carefully research the answers, and engage as many individuals as possible in setting up the network and ensuring the evolving requirements meet the needs of the emergency response community, both today and in the future.

Myth	Reality
Wireless broadband will make our LMR systems obsolete as soon as we turn it on.	LMR voice communications are the backbone of public safety and will be around for years. The current capabilities of wireless broadband make it a valuable addition to LMR as a communications tool for emergency responders.
Once you set up your public safety broadband network, you can share as much high-definition video you want with anyone.	Video will be available to emergency responders on a nationwide network, but how much, how often, and discussions about what should be shared, with whom, and when need to occur. DHS, NIST, and other stakeholders are developing standards through the Video Quality in Public Safety working group.
Agencies will be able to instantly share information with anyone, at any time, once the broadband network is established. All information will flow seamlessly across the network to everyone (text, computer-aided dispatch, e-mail, etc.).	Thoughtful and careful planning is essential. Prior to information sharing within a region, agencies must consider the type of information to share, the owners of that information, the applications needed, and the governance agreements or MOUs that must be established in order to share the information. A good deal of planning needs to occur; there is no "flip of a switch" where everything works and information is shared. The key elements include planning, design, and specifications.
Wireless broadband will solve all public safety problems.	Emerging technologies are often touted by the media and vendors as 'solving' interoperability. There is no doubt that wireless broadband offers tremendous benefits for public safety. However, it's important for agencies to ensure they remain grounded in their decision of when to deploy. For broadband to work in any area, it must be designed to work in the environment where it will be deployed, which differs from State to State and region to region. The key elements include planning, design, and specifications.
Smartphones and other broadband devices can run many applications, so emergency responders should just use them on their public safety network while at work.	The applications and resources currently available on personal smartphones, laptops, and other portable devices are excellent. However, devices and applications are not currently designed for any sustained use in a public safety environment. Standards, specifications, and cost models need to be worked through before these technologies can be made available and relied upon by public safety. The key elements include planning, design, and specifications.

Appendix A: Implementing Public Safety Wireless Broadband

- ☐ Research available references and best practice examples for wireless broadband use, ideally from your own State.
- ☐ Coordinate with statewide interoperability stakeholders, such as the SWIC, the State CIO, neighboring jurisdictions, any broadband task forces or working groups, and any other public services considering broadband use.
- ☐ Study FCC regulations and document requirements for your wireless broadband network. Consider factors such as:
  - Types of data needed (medical records, mug shots, surveillance video, etc.)
  - Sources of data (banks, hospitals, public records, and many others)
  - Formats used for data (CAD files, video, images, text, etc.)
  - Security required for sensitive information, such as law enforcement data or medical files.
  - Reliability and durability of the network during adverse events.
  - Chain of custody for captured/transferred data. As with best practices for capturing data now, your digital data network should show the chain of custody in the event of a subpoena.
  - Prioritization of communications; with self-constructed public safety LMR, incident commanders are accustomed to prioritizing different groups depending on their criticality and communications needs. This prioritization takes on added complexity when applied to a wireless broadband network.
- ☐ Determine your approach to constructing the wireless broadband network.
  - Consider how to meet local needs while complying with FCC regulations.
  - Will you build your own network or purchase service from a commercial vendor?
    - If building your own network, take steps to secure spectrum access.
  - Will your network be limited to your own agency or jurisdiction, or will you try to incorporate a wider network of subscribers?
- ☐ If releasing an RFP for the construction of a public safety network, be sure to include all requirements. If possible, review RFPs released by other public safety entities for wireless broadband.
  - If purchasing service from an existing commercial vendor, be sure to negotiate for the mission critical requirements needed by your subscribers, as they will likely differ from typical subscriber requirements.
- ☐ Explore the funding sources available. Be sure to talk with other emergency responder groups to understand the true cost of supporting a wireless broadband network, particularly the equipment upgrades associated with a rapidly-evolving technology.
  - Will the network be self-supported?
  - If using grant funding for startup costs, how will the ongoing costs of system maintenance and equipment upgrades be paid for after the grant runs out?

Appendix B: Wireless Broadband Fundamentals

Emergency responders today need more information than their traditional radio can provide–everything from building floor plans to live surveillance video. The mobile environment in which public safety works requires wireless broadband capabilities that can operate across a range of frequencies. Although wireless broadband is available to a certain degree commercially–in some areas that is the only option–many agencies plan to build their own wireless broadband networks to public safety specifications.

The Federal Communications Commission (FCC) has adopted Long Term Evolution (LTE) as the standard technology for use on 700 MHz public safety broadband networks.

- The FCC's Emergency Response Interoperability Center is leading the effort to define technical interoperability requirements for wireless broadband, in close coordination with the sole national licensee for public safety broadband, the Public Safety Spectrum Trust (PSST), the National Institute of Standards and Technology, emergency response organizations, waiver jurisdictions, and the broader emergency response community.
- The FCC granted waivers to 21 jurisdictions to begin building 700MHz broadband networks. These waiver jurisdictions have FCC permission to lease spectrum under the PSST's national license to plan and build their networks, but must comply with all FCC orders and any future rules and regulations.

Interoperability Planning for Broadband: Key Takeaways

It is imperative to involve interoperability stakeholders, such as Statewide Interoperability Coordinators, in wireless broadband discussions and to involve wireless broadband stakeholders in interoperability conversations.

- In the near term, wireless broadband will complement land mobile radio (LMR) voice networks, not replace it.
  - Wireless broadband networks are maturing as a valuable addition to LMR, but do not have the reliability, talk around, guaranteed access, and other mission critical qualities that would allow them to currently replace LMR voice communications.
- Consider system life cycle costs.
  - Funding to launch wireless broadband projects can be difficult to obtain. Emergency response agencies should also anticipate the ongoing system maintenance and equipment upgrade costs of a fast-evolving technology.
- Education and outreach are critical to help wireless broadband efforts.
  - As with most existing public safety networks, many broadband networks will ultimately be financed by taxpayer dollars. Taxpayers and elected officials who have a basic knowledge of broadband and the benefits it offers emergency response are much more likely to support broadband.
- Many States and regions already have established governance structures. Every effort should be made to fold wireless broadband projects into these structures, rather than establishing separate governance bodies.
  - The groundwork for statewide governance should be laid as soon as possible; once funding becomes available, governance will be that much harder to establish.
  - Wireless broadband capabilities should be incorporated into the Statewide Communication Interoperability Plan and other interoperability planning documents.

Appendix C: Organizations Working on Nationwide Public Safety Broadband

This Appendix serves as a resource for Statewide Interoperability Coordinators (SWICs) to help in information gathering and planning efforts, and to track activities involving organizations engaged in nationwide broadband issues and the build-out of a nationwide public safety wireless broadband network.

As a testament to the importance of nationwide broadband for public safety and the imperative that the new network be interoperable, a number of Federal programs and organizations, as well as professional organizations are actively responsible for and/or working aggressively on the issue.

Although this is by no means an exhaustive list of all organizations and associations working actively on public safety broadband, it is representative of those that directly touch the emergency response community. Wherever possible, links have been provided to enable ease of access to additional information and materials.

Federal Communications Commission

The Federal Communications Commission (FCC) is responsible for regulating communications by radio, television, wire, satellite, and cable throughout the United States and its possessions. In April 2010, the FCC established the *Emergency Response Interoperability Center (ERIC)* within the FCC Public Safety and Homeland Security Bureau. ERIC is working in tandem with the Department of Commerce's (DOC) *Public Safety Communications Research (PSCR) program* regarding the development of the nationwide public safety wireless broadband network.

ERIC is supported by a Technical Advisory Committee made up of stakeholder representatives from the emergency response community with expertise in the areas of interoperability, network engineering, network governance, technical standards, and policy development. ERIC is also supported by a *Public Safety Advisory Committee (PSAC)*, which is providing guidance to ensure the overarching goal of interoperability in the public safety broadband network is met. The PSAC is assisting ERIC with:

1. Technical and operational requirements to ensure a nationwide level of interoperability.
2. Requirements and procedures to address operability, roaming, priority access, and other matters related to the functioning of the public safety network.
3. Authentication and encryption requirements for common public safety applications and network use.
4. Coordination of ERIC's policies with other entities, including other Federal agencies.

FCC filings related to the *nationwide public safety broadband network* and related 700 MHz spectrum (e.g., quarterly reports from waiver jurisdictions, notices of filing, comments, ex parte communication), are available on the FCC's website at *http://fjallfoss.fcc.gov/ecfs/comment_search/input?z=vzbo8* and enter Proceeding Number 06-229.

National Public Safety Telecommunications Council (NPSTC)

As a volunteer federation of 15 public safety organizations, liaising with Federal agencies including but not limited to DOC, the Department of Homeland Security (DHS), the Department of Interior, the Department of Justice (DOJ), and the FCC, the *NPSTC* has sought to monitor and study public policy, and submit comments to governmental organizations on behalf of public safety. Since September 11, 2001, NPSTC has had a significant role in influencing national policy and regulatory issues regarding interoperability and wireless broadband communications.

NPSTC has been heavily engaged in the developing nationwide public safety broadband network, creating a Broadband Task Force (BBTF) to develop minimum recommendations necessary to support roaming and interoperability among the waiver entities; NPSTCs Executive Council issued a BBTF Report with the recommendations in August 2009.

Public Safety Communications Research Program (PSCR)

The PSCR program is a public safety practitioner driven research and development entity jointly managed by the National Institute of Standards and Technology Office of Law Enforcement Standards and the National

Telecommunications and Information Administration (NTIA) Institute for Telecommunication Sciences of the DOC.

Through the PSCR program's laboratories in Boulder, Colorado, it is providing leading edge research, development, testing, and evaluation of emerging technologies, equipment and services for first-responder communications capabilities. Drawing on critical requirements provided by public safety practitioners, the PSCR program provides insight to wireline and wireless standards committees developing standards for voice, video, and data, communications. The PSCR program is currently involved in various study items supporting the development of the nationwide public safety wireless broadband network.

Public Safety Spectrum Trust

On November 17, 2007, the *Public Safety Spectrum Trust (PSST)* was selected by the FCC as the sole Public Safety Broadband Licensee (PSBL) for 10 MHz of the 700 MHz public safety nationwide broadband spectrum. As a 501c (3) organization, PSST provides the structure and leadership by which decisions on nationwide public safety can guide the construction and operation of an interoperable nationwide public safety-grade broadband network.

The PSST established the Operator Advisory Committee to facilitate communication and coordination among the 21 waiver entities. This working group hosts a weekly conference call for sharing information among the waiver jurisdictions and the PSST and to interface with staff from DOJ, the Office of Emergency Communications (OEC), PSCR, NTIA, and other members of the emergency response community.

Regional Planning Committees

In addition to the 700 MHz PSBL, in 1998 the FCC established *Regional Planning Committees (RPCs)* comprised of public safety stakeholders and radio engineers to help them plan how to use the 700 MHz narrowband spectrum within the region, encourage innovative use of the spectrum, and accommodate new and as yet unanticipated developments in technology and equipment.[3]

Each of the 55 RPCs is required to submit a plan for the General Use spectrum and must ensure the proposed plans comply with all rules and policies governing 700 MHz.[4] The FCC's role in relation to the RPCs is limited to (1) defining the regional boundaries; (2) requiring fair and open procedures, i.e., requiring notice, opportunity for comment, and reasonable consideration; (3) specifying the elements that all regional plans must include; and (4) reviewing and accepting proposed plans (or amendments to approved plans) or rejecting them with an explanation.

Additional details on the RPC, including an *RPC Directory and RPC Interactive Map* on the *Public Safety and Homeland Security Bureau link*, are available on the FCC website. As part of statewide outreach and coordinating planning efforts, SWICs should consider connecting with their respective RPC to plan and utilize 700 MHz narrowband spectrum in their State.

3 See Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, WT Docket No. 96-86, *First Report and Order and Third Notice of Proposed Rulemaking*, 14 FCC Rcd 152 (1998) (*First Report and Order*); *Second Memorandum Opinion and Order*, 15 FCC Rcd 16844 (2000). See also 47 C.F.R. § 90.527.

4 *See* 47 C.F.R. § 90.527. Each RPC must incorporate certain common elements into its 700 MHz plan. A list of 700 MHz RPCs and region activities is available at *http://www.fcc.gov/pshs/public-safety-spectrum/700-MHz/*.

Appendix D: Broadband Grants and Resources

Wireless Broadband Grant Opportunities

As stakeholders turn to emerging technologies such as broadband, wireless data networks, Internet Protocol (IP)-based mobile communications devices, and location-based commercial services to meet interoperable and emergency communications challenges, they increasingly are looking for Federal grant programs that can help fund these initiatives. The *FY 2011 SAFECOM Guidance on Emergency Communications Grants* developed by the Office of Emergency Communications provides guidance on broadband planning under these grant programs. Several grant programs are intended to be one-time funding programs. However, implementing broadband projects for these grant programs may still be in progress.

Grant Programs Funding Broadband Technologies

The list below is of grant programs that fund broadband activities and a short description of each program. A website is provided for more information.

- Border Interoperability Demonstration Project (BIDP)
- Broadband Initiatives Program (BIP)
- Broadband Technology Opportunities Program (BTOP)
- Emergency Management Performance Grant (EMPG)
- E911 Grant Program
- Freight Rail Security Grant Program (FRSGP)
- Homeland Security Grant Program (HSGP) (FY 2011)
- Interoperable Emergency Communications Grant Program (IECGP)
- Public Safety Interoperable Communications (PSIC) Grant Program

Border Interoperability Demonstration Project (BIDP)—One-time grant program

BIDP is a one-time, competitive demonstration project that provides funding to State, local, and tribal entities to develop and identify innovative approaches to improving interoperable emergency communications along and across U.S. international borders.

Agency: DHS/OEC

Website: *http://www.dhs.gov/xopnbiz/grants/gc_1261517564250.shtm*

Broadband Initiatives Program (BIP)

The purpose of Broadband Initiatives Program is to award grants, loans, and loan/grant combinations for the purpose of facilitating broadband deployment in rural communities. This is a one-time program funded through the American Reinvestment and Recovery Act.

Agency: USDA/RUS

Website: http://www.broadbandusa.gov

Broadband Technology Opportunities Program (BTOP)

The purpose of BTOP is to provide improved access to broadband service to consumers residing in unserved and underserved areas of the U.S.; provide broadband education, awareness, training, access, equipment, and support to community anchor institutions, organizations that support vulnerable populations, or job-creating strategic facilities in economic development zones; improve access to, and use of, broadband service by public safety agencies; and stimulate the demand for broadband, economic growth, and job creation. Seven of the 21 FCC waiver jurisdictions have received roughly $380M in BTOP funding to construct wireless broadband networks for public safety.

Agency: Department of Commerce (DOC)/NTIA

Website: *http://www.broadbandusa.gov*

Emergency Management Performance Grant (EMPG)

The EMPG assists State and local governments in enhancing and sustaining their all-hazards emergency management capabilities. The EMPG supplemental provided an additional $50 million to assist State and local governments to sustain and enhance all-hazards emergency management capabilities.

Agency: DHS/FEMA

Website: *http://www.fema.gov/government/grant/empg/index.shtm*

E911 Grant Program

The purpose of the e-911 Grant Program is to provide funding for the implementation and operation of Phase II enhanced 911 services and for migration to an Internet Protocol (IP)- enabled emergency network.

Agency: DOT/NHTSA

Website: *http://www.e-911ico.gov/*

Freight Rail Security Grant Program

The Freight Rail Security Grant Program will fund freight railroad carriers and owners and offerors of railroad cars to protect critical surface transportation infrastructure from acts of terrorism, major disasters, and other emergencies.

Agency: DHS/FEMA

Website: *http://www.fema.gov/government/grant/frsgp*

Homeland Security Grant Program (HSGP)

The HSGP is comprised of five interconnected grant programs: State Homeland Security Program (SHSP), Urban Areas Security Initiative (UASI), Operation Stonegarden (OPSG), Metropolitan Medical Response System (MMRS), and Citizen Corps Program (CCP). The FY 2011 HSGP supports emergency communications activities to include the purchase of interoperable communications equipment and technologies such as voice-over-internet protocol bridging or gateway devices, or equipment to support the build out of wireless broadband networks in the 700 MHz public safety band under the Federal Communications Commission Waiver Order. To purchase equipment, the grantee must ensure that projects support the Statewide Communication Interoperability Plan (SCIP) and are fully coordinated with the Statewide Interoperability Coordinator (SWIC) in the State of the project. Grantees (and sub-grantees) are required to provide the Authorized Equipment List (AEL) number for all communications equipment purchased with grant award funding (plus a description of the equipment and the quantity purchased of each item) to the FEMA GPD once items are procured as part of periodic programmatic grant reporting.

Agency: DHS/FEMA

Website: *http://www.fema.gov/government/grant/hsgp/index.shtm*

Interoperable Emergency Communications Grant Program (IECGP)

IECGP provided funding to State, local, and tribal entities for governance, planning, training, and exercise funding to States, territories, and local and tribal governments to carry out initiatives to improve interoperable emergency communications, including communications in collective response to natural disasters, acts of terrorism, and other man-made disasters. Although this grant has been defunded for FY 2011, projects approved for this funding in the FY 2010 Appropriations bill are still ongoing through 2013.

Agency: DHS/FEMA/OEC

Website: *http://www.fema.gov/government/grant/iecgp/index.shtm*

Public Safety Interoperable Communications (PSIC) Grant Program—One-time grant program.

The PSIC Grant Program provided one-time funding to States and territories to enable and enhance public safety agencies' interoperable communications capabilities.

Agency: DOC/NTIA

Website: *http://www.ntia.doc.gov/psic*

Broadband and Reference Materials

1. *Emergency Communications System Life Cycle Planning Guide*
2. *Formal Agreement and Standard Operating Procedure Template Suite and Reference Library*
3. *National Broadband Plan*
4. *National Emergency Communications Plan (NECP)*
5. *National Public Safety Telecommunications Council (NPSTC)*
6. *Law Enforcement Tech Guide for Communications Interoperability*

Appendix E: Acronyms and Common Terminology

3G	Third Generation
APCO	Association of Public-Safety Communications Officials—International
BTOP	Broadband Technology Opportunity Program
DHS	Department of Homeland Security
DOC	Department of Commerce
DOJ	Department of Justice
EMS	Emergency Medical Services
ERIC	Emergency Response Interoperability Center
FCC	Federal Communications Commission
IP	Internet Protocol
LMR	Land Mobile Radio
LTE	Long Term Evolution
MHz	Megahertz (Million Hertz)
NG911	Next Generation 911
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OAC	Operator Advisory Committee
OEC	Office of Emergency Communications
PSBL	Public Safety Broadband License
PSCR	Public Safety Communications Research
PSHSB	Public Safety and Homeland Security Bureau
PSST	Public Safety Spectrum Trust

SAFECOM is a communications program of the Department of Homeland Security. SAFECOM provides research, development, testing and evaluation, guidance, tools, and templates on interoperable communications-related issues to local, tribal, state, and Federal emergency response agencies. The Office of Emergency Communications (OEC) supports SAFECOM's development of grant guidance, policy, tools, and templates, and provides direct assistance to local, tribal, state, and Federal practitioners. The Office for Interoperability and Compatibility (OIC) supports SAFECOM's research, development, testing and evaluation, standards, and tools such as reports and guidelines. OEC is an office within the Directorate for National Protection and Programs. OIC is an office within the Science and Technology Directorate.

Visit www.safecomprogram.gov or call
1-866-969-SAFE