Public Safety Communications Evolution

May 2014

Homeland
Security

Public Safety Communications Evolution

The Department of Homeland Security's Office of Emergency Communications (OEC) developed this brochure in collaboration with SAFECOM and the National Council of Statewide Interoperability Coordinators, with the support and input of public safety officials at multiple levels of government across the country. This brochure:

1. Helps educate the public safety community and elected and appointed officials about the future of emergency communications
2. Describes the evolution of emergency communications and how traditional land mobile radio (LMR) communications used today may converge with wireless broadband in the future, if specific requirements are met
3. Discusses some of the most important requirements to achieve the desired long term state of convergence with LMR networks

The public safety community made significant strides toward strengthening national preparedness and improving emergency communications capabilities. First responders, however, continue to be limited by fragmented networks and decades-old wireless technologies. Deploying a cost-effective, nationwide public safety wireless broadband network will provide public safety agencies with access to advanced, cutting edge technologies and applications to improve their emergency response capabilities. In February 2012, the Middle Class Tax Relief and Job Creation Act (Public Law 112-96) authorized the development and implementation of the Nationwide Public Safety Broadband Network (NPSBN). The law also establishes the First Responder Network Authority (FirstNet) as an independent body that governs the NPSBN; sets aside $7 billion for network development, deployment, and operation; and assigns the use of the 700 MHz D Block to FirstNet for the public safety community. As envisioned, the network will incorporate open, commercial wireless technology standards.

As promulgated by statute, FirstNet is led by a 15-member Board, which includes the Secretary of Homeland Security, the Attorney General of the United States, and the Director of the Office of Management and Budget. The additional 12 members have broad experience in public safety, technology, and telecommunications networks development. In addition, the statute requires more representation of States, tribes, territories, or rural and urban areas.

http://www.ntia.doc.gov/page/about-firstnet

The NPSBN needs to be closely aligned with the commercial deployments of Long Term Evolution (LTE) wireless services to keep pace with changes in technology and to leverage cost efficiencies. It must embrace levels of availability and robustness found in today's public safety LMR mission critical voice networks to deliver wireless data communications services to public safety agencies in Federal, State, local, tribal, and territorial (F/S/L/T/T) jurisdictions across the Nation, as well as to Federal responders and secondary users (such as transportation, public services/public works, and utilities). If there is a convergence of LMR mission critical voice to broadband, F/S/L/T/T and private sector entities must work together to develop requirements and standards to assure mission critical voice and data operations.

In the near term, wireless broadband will complement LMR, not replace it. Commercially available wireless broadband services do not currently meet the requirements for emergency response voice communications; therefore, LMR will remain as the primary voice communications service for public safety for the foreseeable future.

Investments in LMR will continue to be necessary now and well into the future. Public safety's use of LMR systems will continue for the foreseeable future as there is no defined timeframe when LTE broadband technology may provide the same level of mission critical voice services that are available today. Therefore, it will be necessary to continue investments for existing and new LMR voice systems, while allocating new funding to the development and deployment of the NPSBN.

Public safety is using commercial broadband services today for many different data applications (e.g., National Crime Information Center/State Criminal Justice Information Systems queries, Computer-Aided Dispatch information, Records Management System queries, location based information, picture and image transmission), but not for mission critical emergency response voice communications. Although initial data applications will not provide mission critical LMR type voice services, these data applications are vital and can dramatically improve emergency response and the provision of public safety services.

In the future, broadband may be able to support mission critical voice. However, requirements must be developed, technical standards created and accepted, and new equipment and services built and tested for operational readiness and compliance in the challenging public safety environment. Until broadband is technically capable of supporting public safety mission critical voice communications and the NPSBN is fully deployed, public safety agencies will need to continue to use current LMR networks for their mission critical voice communications.

Public Safety Communications Today

Currently, the public safety community relies on LMR systems to support mission critical voice communications. These radio systems provide a reliable means for personnel in the field to communicate with each other, with public safety answering points (PSAPs), and with communications centers. As LMR systems evolved, a number of varying, and often incompatible, systems came into use nationwide. As a result, public safety has struggled with interoperability, the ability to facilitate communications across jurisdictional and agency lines.

In addition, public safety agencies continue to use a combination of low bandwidth LMR and high-speed broadband data services (largely commercial networks) to support response efforts and perform wireless data access functions such as digital dispatch, license plate queries, text messaging, and transmission of low resolution images. While important, the majority of current wireless broadband data solutions are limited in their ability to support emergency responders because many are not interoperable, do not embrace public safety standards and practices for robustness and resiliency, and do not incorporate high availability network components to enhance accessibility.

There are a growing number of applications being developed to support public safety, including:

- Automatic Vehicle Location (AVL) and in vehicle navigation
- Incident Command White Board
- Real-time fixed and mobile video (receipt and transmission)
- Shared video and real time camera resources available from non-government entities, such as alarm companies, security offices, complexes, building and facilities, and other commercial and private establishments etc.
- Mobile Data Computing
- Patient, Evacuee, and Deceased Persons Tracking
- Sensor Monitoring and Manipulation (M2M)
- Geographic Information System (GIS) access

What is Wireless Broadband?

Wireless broadband provides high-speed data communications in a mobile environment. Because of public safety's unique mission, emergency responders require wireless broadband services and devices with prioritized access and the highest levels of reliability, coverage, and security not currently offered by commercial systems.

The Nationwide Public Safety Wireless Broadband Network

By providing mobile access to real-time, multimedia information, the goal of the NPSBN is to drastically improve the public safety community's ability to communicate with response agencies, regardless of jurisdiction, in an effort to access vital information. For example, public safety will be able to watch video images of a crime in progress, download building plans of a burning building to a handheld device, or connect rapidly and securely with personnel from other towns and cities. Just as smart phones have changed the way society communicates, these technology advancements will dramatically change the way emergency responders communicate and operate.

Advances in wireless data communications are increasing mobile access to applications and providing real-time information needed by public safety. Whether used in routine, daily activities or large-scale responses, these new capabilities will improve emergency communications and response effectiveness. For example, Advanced Automatic Crash Notification provides pre-arrival information to hospitals and enables responders to make faster and well-informed decisions about resources to send to a scene. This allows for faster diagnosis and treatment of patients by Emergency Medical Technicians (EMT) or even a virtual physician in the back of the ambulance to expedite proper lifesaving treatment.

The Advanced Automatic Crash Notification example demonstrates how wireless broadband applications could provide instant, actionable knowledge to emergency response personnel. The right information (such as weather reports, wanted persons and vehicles, hazardous material information, drivers' licenses and photos, criminal history records, incident scene pictures/video) provided to the right people at the right time will result in more effective emergency response. These and other emergency response applications are only possible with high-speed wireless broadband.

While the public safety community has long recognized the importance of wireless broadband services, they also recognize certain challenges must be overcome and requirements must be met for this technology to meet all of their communications needs. It will take time to address these requirements and integrate wireless broadband into public safety operations. If these requirements are met, the NPSBN will dramatically enhance the capabilities of emergency responders in the future. [1]

The Nationwide Public Safety Wireless Broadband Network will allow first responders to match a subject's photograph (taken with a smartphone or Tablet PC) against databases such as the Department of Motor Vehicles or booking databases to determine identity.

What about the SAFECOM Interoperability Continuum?

The five critical success elements in the SAFECOM Interoperability Continuum (Governance, Standard Operating Procedures, Technology, Training and Exercise, and Usage) are important to consider when planning and implementing interoperability solutions for all public safety communications technologies. The Continuum will continue to be used as a guiding framework for interoperability planning for the NPSBN.

[1] United States, White House, The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety, June 2011.

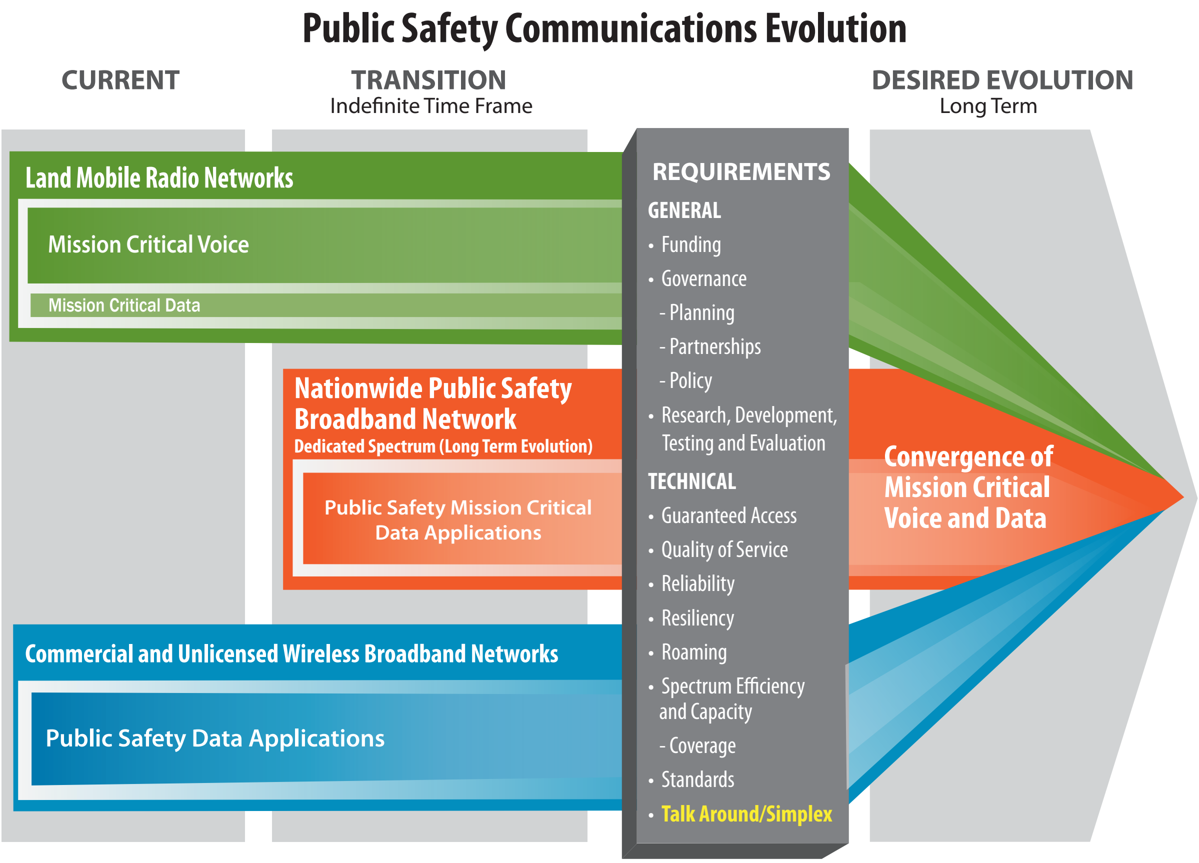
Public Safety Communications Evolution
CURRENT
TRANSITION
Indefinite Time Frame
DESIRED EVOLUTION
Long Term
Land Mobile Radio Networks
Mission Critical Voice
Mission Critical Data
Nationwide Public Safety Broadband Network
Dedicated Spectrum (Long Term Evolution)
Public Safety Mission Critical Data Applications
Commercial and Unlicensed Wireless Broadband Networks
Public Safety Data Applications
REQUIREMENTS
GENERAL
• Funding
• Governance
- Planning
- Partnerships
- Policy
• Research, Development, Testing and Evaluation
TECHNICAL
• Guaranteed Access
• Quality of Service
• Reliability
• Resiliency
• Roaming
• Spectrum Efficiency and Capacity
- Coverage
• Standards
• Talk Around/Simplex
Convergence of Mission Critical Voice and Data

Figure 1: This graphic illustrates a public safety communications evolution by describing the long-term transition toward a desired converged future.

Public Safety Communications Evolution

The vision of the evolution of public safety communications as it transitions from today's technology to the desired long-term state of convergence is shown in the graphic above (Figure 1). This figure outlines a conceptual framework for deploying nationwide wireless broadband communications while maintaining LMR networks to support mission critical voice communications. This section of the brochure describes the elements of this framework in more detail, including a description of the desired converged environment and the requirements that must be met to achieve this desired evolution.

In the current state of communications, LMR networks, commercial broadband networks, and the NPSBN 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 continue to implement emerging wireless broadband services and applications. During the transition period, FirstNet, in conjunction with public safety, will begin building out the NPSBN and public safety organizations will begin to transition from commercial broadband services to the dedicated public safety network. If and when the technical and non-technical requirements are met and are proven to achieve mission critical voice capability, it is anticipated that agencies will migrate partially or entirely to this broadband technology. Since wireless broadband technology does not currently support a mission critical voice capability (i.e., talk around/simplex/direct mode), there will be a significant period of time where wireless broadband networks and LMR systems are necessary.

Land Mobile Radio Networks

Mission critical voice communications have historically been delivered using LMR systems built to public safety requirements and operated by individual agencies or jurisdictions.

Mission Critical Voice

Reliable voice communications are essential for day-to-day operations, large-scale responses, and other tactical situations. Voice communications provide emergency responders with instant, reliable, and continuous connectivity between dispatch agencies and responders and also among multiple responders. Presently, mission critical voice is achieved by dedicated LMR networks. The ability to talk responder-to-responder or one responder to many responders is a critical feature.

Mission Critical Data

The emergency response community uses data communications to complement mission critical voice communications. Emergency responders currently use data services for basic functions, such as digital dispatch; license, vehicle, and wanted person queries; text messaging; and transmission of low resolution images. Emergency response agencies have achieved wireless data capabilities by either building their own systems, by using commercial wireless service providers, or a combination of both.

Although functional, current public safety data services are generally limited in speed, coverage, and capacity and do not support advanced, real-time applications needed by emergency responders.

Nationwide Public Safety Broadband Network

Public safety envisions the NPSBN as a dedicated network built to public safety requirements using dedicated and allocated 700 MHz spectrum. The public safety community and the Middle Class Tax Relief and Job Creation Act of 2012 (PL 112-96) identified LTE as the technology standard for development of this network. As this capability is built using LTE technology, public safety will continue to work with industry and all levels of government to advance the technology and address the requirements necessary to reach the desired evolution. During the transition period, public safety will begin using LTE for mission critical data applications.

Commercial and Unlicensed Wireless Broadband Networks

Emergency responders are increasing the use of commercial broadband networks to augment their mission critical voice communications. Although not built to public safety standards, commercial networks are valuable because they complement reliable public safety LMR voice networks. As commercial wireless broadband capabilities are made available, public safety agencies are using these services to complement their current LMR communications. Agencies will use their LMR networks for mission critical voice communications, and will increasingly use commercial wireless broadband for critical data communications. Over time, reliable public safety broadband networks based on LTE technology will be built to public safety requirements. As the NPSBN is implemented, real-time mission critical broadband applications will migrate to this network as their capabilities are validated by responders.

Requirements

General and technical requirements must be met for the desired evolution to be achieved.

General Requirements

Funding

Emergency response agencies continue to face the challenge of funding their current mission critical voice systems while planning for the deployment of emerging technologies, including wireless broadband. A business plan is being developed by FirstNet to identify, define, and delineate the costs associated with the implementation and sustainment of the NPSBN. As a part of the business planning process, various funding models and revenue streams including the imposition of user/subscriber fees for services may be considered.

As a part of PL 112-96, Congress allocated $7 billion in overall funding for the development, construction, operation, and management of the envisioned NPSBN. This funding will be accumulated from spectrum auctions conducted by the Federal Communications Commission (FCC) and placed into the public safety trust fund. Of the $7 billion, $2 billion has been borrowed from the U.S. Treasury in order to be immediately available to the National Telecommunications and Information Administration (NTIA) for the startup of FirstNet and initial network deployment and operational expenses. Additionally, $135 million, reduced to $118.5 million after sequestration, has been allocated to the State and Local Implementation Grant Program (SLIGP) as a formula-based, matching grant program administered by the NTIA. The program is designed to assist F/S/L/T/T and regional government entities as they plan for the NPSBN.

Governance–Planning, Partnerships, and Policy

Coordination and collaboration among interoperable communications stakeholders makes the success of any governance structure possible. As provided in PL 112-96, FirstNet has initiated the development of the NPSBN architecture and created a governance structure.

In addition to FirstNet's technical and managerial efforts for the NPSBN, effective governance requires the active engagement of emergency communications stakeholders operating at the F/S/L/T/T levels, across jurisdictions and disciplines.

Planning: It is critical that public safety stakeholders engage in nationwide, statewide, regional, and tactical planning. Planning and coordination among entities, such as Statewide Interoperability Coordinators, Statewide Interoperability Governing Bodies, Regional Interoperability Councils, and Federal partners form an essential foundation for achieving statewide communications interoperability goals and initiatives.

Partnerships: As wireless broadband communications evolve, partnerships will continue to be critical, particularly with respect to developing and deploying the NPSBN that aligns and leverages existing governmental and commercial infrastructure and services. Further, the development of the NPSBN will require close coordination and partnering between industry and government. Public safety agencies need to evaluate their governance bodies to ensure they include those stakeholders that rely on and deliver communications during emergencies as well as industry subject matter experts. The partnerships built through governance provide agencies with access to knowledge (e.g., best practices and lessons learned) and resources previously unavailable.

Policy: It is critical for all levels of government to proactively and collaboratively develop policies and plans for emerging emergency communications technologies. With the establishment of FirstNet, there is a nationwide governance structure that will collaborate with F/S/L/T/T agencies to develop new initiatives, strategies, and time frames related to investments and deployment of the NPSBN. FirstNet has also established the Public Safety Advisory Committee to assist FirstNet in carrying out its duties and responsibilities.

Research, Development, Testing, and Evaluation (RDT&E)

RDT&E efforts will ensure that emergency responders have reliable, effective, standardized, and interoperable wireless broadband capabilities and applications. Research and development are critical to determine how systems will meet emergency response requirements, and if these capabilities will sustain reliability and functionality in the harsh environments in which emergency responders often work.

Technical Requirements

OEC continues to work closely with the public safety community to establish and refine a set of technical and operational requirements and priorities for public safety wireless broadband systems. These elements were developed by those stakeholders with the understanding that as the NPSBN evolves, the emergency response community will increasingly leverage the capabilities of the NPSBN to support their operations. To achieve a converged evolution end state, the NPSBN will need to support the following technical requirements:

Guaranteed Access

Emergency responders must have guaranteed access to reliable and instantaneous communications at all times to effectively respond to emergency incidents. Guaranteed access is a critical feature for public safety, especially when using commercial networks.

Quality of Service (QoS)

Public safety requires a broadband network that will guarantee a high level of performance for critical applications. As all public safety communications move toward a converged broadband wireless environment, some data on the network will be more important than others and will need to be prioritized. In a network, QoS specifies how certain types of data are handled and how that data is prioritized among various users and applications. QoS ensures reliable performance.

Reliability

For emergency responders to be able to rely on the NPSBN for mission critical communications, it must be designed to minimize capacity loss and service degradation.

Resiliency

Systems that support emergency response must be developed with resiliency in mind. Highly reliable and redundant power, components, infrastructure, and communication paths must be included to reduce the possibility of disruption in service.

Roaming

To perform their jobs efficiently, emergency responders require the ability to seamlessly roam between public safety and commercial networks, as necessary.

Spectrum Efficiency and Capacity

The rapid growth of wireless, broadband-enabled applications and services has placed constraints on available spectrum capacity in the commercial marketplace, sometimes rendering commercial networks slow and unresponsive. This has major implications for emergency responders who require rapid and reliable access to information in order to successfully accomplish their missions. As provided in PL 112-96, sufficient capacity and spectrum should be available with the 20 MHz of 700 MHz spectrum allocated to the NPSBN to meet the emergency response community's needs. In addition, FirstNet will be working to establish the best available wireless signal coverage that ensures reliable operations in wide geographic regions, including major population centers as well as rural areas.

Standards

Defining technical standards is critical to ensuring that interoperability and public safety-specific features are built into the NPSBN. Standards-based systems will provide backward compatibility, allowing emergency responders to continue to communicate effectively on their current mission critical voice systems as wireless broadband networks and applications mature and are integrated into existing systems. LTE is a worldwide technology standard widely adopted by commercial network operators for their next generation deployments. The FCC, in conjunction with a consortium of public safety associations, also has endorsed the use of LTE in next generation public safety networks. The LTE standard has evolved based on commercial requirements; however, there are ongoing efforts to enhance the standard to meet the public safety community's needs. Difficulties lie in public safety's ability to influence a global standard, such as LTE, because emergency responders represent a small percentage of the LTE consumer market.

Talk Around/Simplex/Direct Mode

Talk around, also known as simplex or direct mode, is the capability to communicate device-to-device when out of range of a wireless network infrastructure or when working in an area where direct unit-to-unit communications is required. This is an important feature for public safety operations as it allows a group of responders to choose to talk directly to each other without the need to connect to the existing network infrastructure. This is a critical capability when the network infrastructure has been damaged or destroyed. For example, when firefighters respond to a wildfire or to an incident in a basement of a burning building that may be outside of any LMR network coverage area, they may use direct mode to continue to communicate with each other despite reduced coverage.

Convergence of Mission Critical Voice and Data

A "converged network" is a dedicated, public safety wireless broadband infrastructure capable of offering mission critical voice, data, and video to emergency responders. It is important because it reduces the costs of developing and maintaining systems and increases the effectiveness of emergency responders in the field. However, convergence will be a long-term proposition and gradual transition as agencies integrate new technologies, rather than replace existing systems. The pace of convergence will vary from agency to agency and will be influenced by operational requirements, existing systems, wireless broadband coverage, and funding levels. During this migration period, solutions for connecting traditional LMR with broadband systems will be necessary. Even when the NPSBN is capable of meeting all public safety voice and data requirements, some agencies may need or choose to operate separate LMR systems. Broadband technology to support mission critical voice is not currently available and it remains too early to define the time frame for the availability of such technology. Therefore, continuing to invest in the sustainment of current LMR networks and deployment of the NPSBN will need to be done simultaneously.

Additional Information and Resources

Administration

- "The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety" (June 2011) http://www.whitehouse.gov/sites/default/files/uploads/publicsafetyreport.pdf
- National Telecommunications and Information Administration, Comments, FCC Docket No. 06-229, "Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band." (June 10, 2011) http://fjallfoss.fcc.gov/ecfs/comment/view?id=6016823007

Association of Public-Safety Communications Officials (APCO) International Public Safety Applications

- http://appcomm.org/

Broadband Outreach Toolkit

- http://www.dhs.gov/publication/broadband-outreach-toolkit

Federal Communications Commission National Broadband Plan

- www.broadband.gov/plan

FirstNet

- http://firstnet.gov/

National Public Safety Telecommunications Council

- Homepage: http://www.npstc.org/
- "Why Can't Public Safety Just Use Cell Phones and Smart Phones for Their Mission Critical Voice Communications?" (April 2013) http://www.npstc.org/download.jsp?tableId=37&column=217&id=2712&file=Why_Cant_PS_Just_Use_Cell_Phones_NPSTC_130415_orig.pdf

National Telecommunications and Information Administration

- http://www.ntia.doc.gov/category/public-safety

Office of Emergency Communications

- Homepage: http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm
- National Emergency Communications Plan: http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf

Public Safety Communications Research Program

- http://www.pscr.gov/

SAFECOM

- Homepage: www.safecomprogram.gov
- Grant Guidance: http://www.safecomprogram.gov/ecg/2013_safecom_guidance_feb_22_final.pdf
- Interoperability Continuum: http://www.safecomprogram.gov/oec/interoperability_continuum_brochure_2.pdf

SAFECOM is a communications program of the Department of Homeland Security and provides feedback and subject matter expertise on interoperable communications-related issues and products to F/S/L/T/T 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.

Homeland Security

SAFECOM

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