Public Safety Communications Evolution

January 2019

CISA
CYBER+INFRASTRUCTURE

Public Safety Communications Evolution

The Cybersecurity and Infrastructure Security Agency (CISA) developed this brochure in collaboration with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), with the support and input of public safety officials at multiple levels of government across the country. The *Public Safety Communications Evolution* brochure:

1. Helps educate the public safety community and elected and appointed officials about the technologies and services to support the future of public safety communications
2. Describes the evolution of public safety communications and how legacy land mobile radio (LMR) communications used today continues to be the primary voice communications pathway for public safety personnel while the First Responder Network Authority's (FirstNet) Nationwide Public Safety Broadband Network (NPSBN) concurrently brings enhanced wireless broadband data communication capabilities through the deployment of a nationwide data network
3. Discusses some of the most important requirements necessary to achieve the desired future long-term evolution of LMR technology networks and whether a transition is beneficial and operationally effective for the public safety community

The public safety community continues to make great strides in improving public safety communications operability and interoperable capabilities while also strengthening responsiveness and preparedness at all levels of government. In February 2012, the Middle-Class Tax Relief and Job Creation Act (Public Law 112-96) authorized the development and implementation of the NPSBN. The law also established the FirstNet Authority as an independent body governing the NPSBN; set aside $7 billion for network development, deployment, and operation; and assigned the use of the 700 MHz D Block to the FirstNet Authority for the public safety community. As envisioned, the network will incorporate open, commercial wireless technology standards.

On March 30, 2017, the FirstNet Authority announced a 25-year public-private partnership agreement with their successful vendor who would be responsible for the deployment and operations of the much anticipated NPSBN with Long Term Evolution (LTE), a worldwide standardized broadband cellular technology. The agreement was the culmination of protracted efforts by the public safety community to bring forth a nationwide public safety interoperable network recommended by the 9/11 Commission after the terrorist attacks of September 11, 2001.

The FirstNet Authority's commercial partner provided a unique approach to meeting the NPSBN's requirements, in which not only would they develop and deploy the network using the dedicated 700 MHz Band 14 spectrum licensed to FirstNet, but also provide access for public safety users to all the commercial carrier's existing LTE spectrum to expand network access and capacity far beyond the 20 MHz of dedicated D block spectrum. The network configuration was augmented with priority and preemption services to ensure unfettered access to the NPSBN resources.

As promulgated by statute, the FirstNet Authority 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

On December 29, 2017, after the release and review of FirstNet's State Plans provided to all 56 states and territories, each Governor had "opted-in," agreeing to have FirstNet and its commercial partner deploy the new network. The public safety community is continuing its use of commercial broadband services through agreements with FirstNet's commercial partner or other commercial wireless carriers to access different data applications and services (e.g., National Crime Information Center/State Criminal Justice Information Systems queries, Computer-Aided Dispatch calls for services information, Records Management System queries, location-based information, picture, video, and image transmission), but not for mission critical voice communications. These data applications and the opportunities to wirelessly connect to other sources of information not previously available are vital and can dramatically improve emergency response, provision of public safety services, and the safety of public safety personnel.

Today, LTE broadband technology provides cellular voice telephony services through the incorporation of Voice over LTE (VoLTE) and commercial carrier offered voice Push-To-Talk (PTT) Over Cellular services (POC). Additionally, other PTT voice services applications are offered in the form of Over the Top (OTT) solutions, via third party vendors, which can provide a degree of PTT interoperability with LMR systems and LTE networks and devices.

However, these presently offered voice capabilities do not operate in the same manner or to the same level of robustness and resilience as what is offered in public safety LMR. Additionally, an OTT solution offered by one vendor may not be interoperable with other OTT solutions operating on other commercial LTE networks.

Various standards development organizations (SDO) continue to collect requirements and engage in processes to craft accredited technical standards for envisioned new equipment and services. Once these standards are ratified by the SDO, manufacturers will produce new equipment and services and commercial carriers will incorporate these new standardized capabilities to be consistent with their technology roadmap for individual networks.

The public safety community will continually need to evaluate and test offered equipment and services to determine operational readiness and compliance in the challenging public safety environment. Until broadband technology is physically and technically capable of supporting public safety voice communications capabilities, consistent with or better than current LMR offerings, public safety agencies at all levels of government will need to continue using current LMR networks for their mission critical voice communications. Wireless broadband voice services will continue to complement and co-exist with LMR, but not replace it. Commercially available wireless broadband voice services do not currently meet all the requirements for public safety voice communications; therefore, LMR will remain as the primary voice communications service for public safety in the foreseeable future. Public safety's use of LMR systems will also 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 available today.

Public Safety Communications Today

The public safety community has relied on LMR systems since the 1930s 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 public safety communications centers. As LMR systems evolved and additional spectrum bands became available, varying and often disparate technologies were developed and deployed in new and upgraded systems across the nation. As a result, the public safety community has struggled with interoperability and the ability to facilitate communications across jurisdictional and agency lines.

In addition, public safety agencies continue to use a combination of low bandwidth LMR data systems and high-speed commercial broadband data services to support response efforts and perform wireless data access functions such as digital dispatch, license plate queries, text messaging, and transmission/receipt of images and video. While significant progress is being made with the implementation of the NPSBN by the FirstNet Authority, many current wireless broadband data solutions are limited in their ability to support public safety responders effectively as they remain non-interoperable, do not embrace public safety standards and practices for robustness and resiliency, and do not incorporate high availability network components to enhance immediate and consistent accessibility.

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

- Automatic Vehicle Location (AVL), Automatic Resources Location (ARL) and in vehicle navigation
- Incident Command Situational Awareness
- Real-time fixed and mobile radio (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, public safety responders require wireless broadband services and devices with prioritized access and the highest levels of reliability, coverage, and security. These capabilities are now becoming mainstream offerings by FirstNet's commercial partner and other commercial broadband network systems operators.

The Nationwide Public Safety Broadband Network

By providing highly available mobile access to a plethora of public safety purpose built application services and information sources, the goal of the NPSBN is to drastically improve the public safety community's ability to communicate with agencies, regardless of jurisdiction or level of government, in an effort to access vital information. For example, public safety can 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 jurisdictions. Just as smart phones have changed the way society communicates, these technology advancements are dramatically changing the way public safety responders communicate and operate.

Advances in wireless data communications are increasing mobile access to applications, facilitating access to more and varied information resources, and providing near real-time information needed by public safety.

Whether used in routine, daily activities or large-scale responses, these new capabilities are improving public safety 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 public safety 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 responses and the provision of timely and efficient public safety services. These and other public safety 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 their communications needs. It will require a continual effort to address these requirements and integrate wireless broadband into public safety operations. As these requirements are met, the NPSBN will dramatically enhance the capabilities of public safety now and in the future.

The Nationwide Public Safety Broadband Network will allow first responders to match a subject's photograph (taken with a mobile device) against Driver's License or Criminal History databases to verify 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.

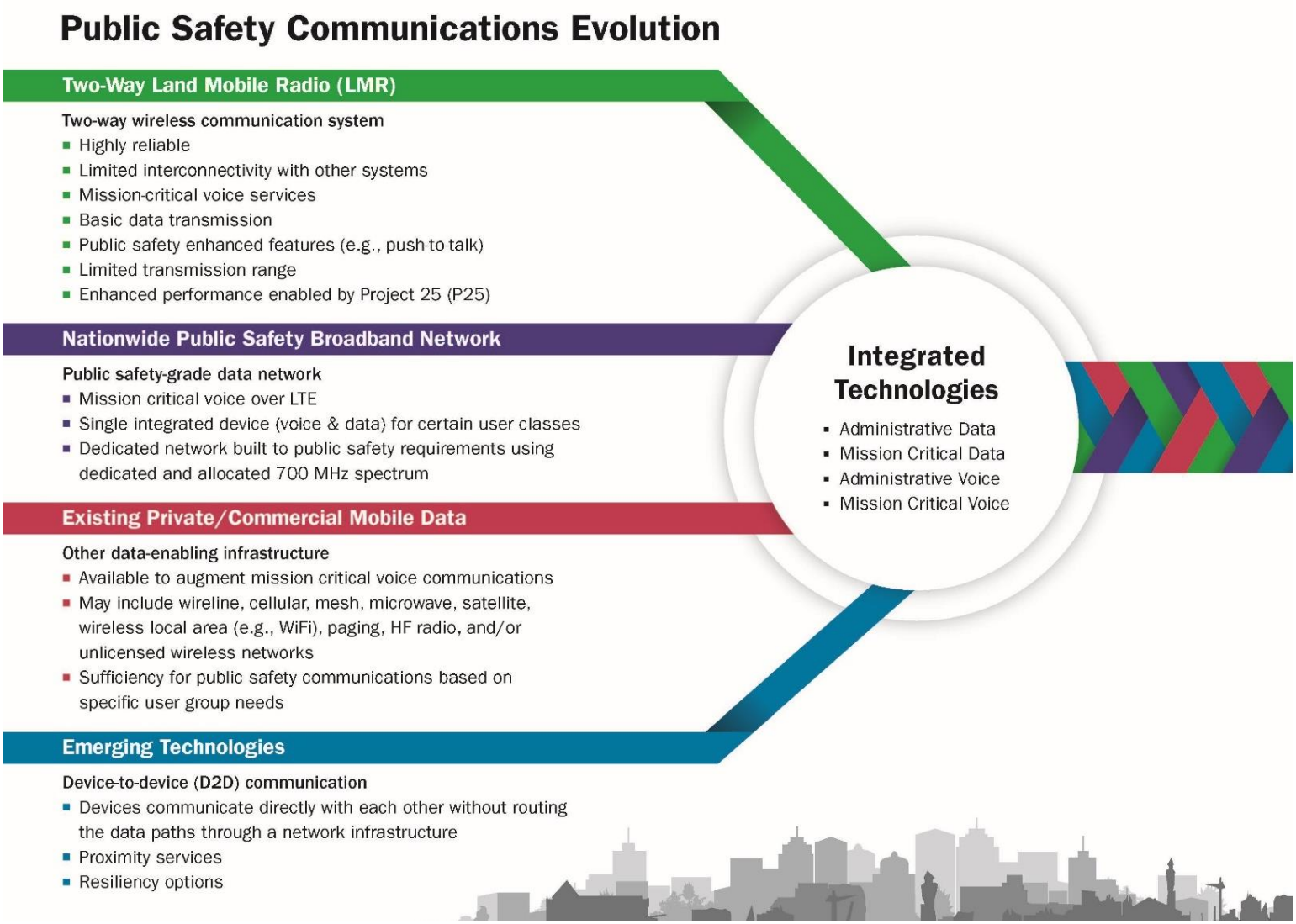


Figure 1: This graphic illustrates public safety communications evolution by describing the long-term transition toward a desired converged future. For more information, please reference "Mission Critical Voice Requirements for Public Safety" *published by the National Public Safety Telecommunications Council at* http://www.npstc.org/npstcReports.jsp.

Public Safety Communications Evolution

The vision of public safety communications as it transitions from today's technology to the desired long-term evolution is shown in the graphic above (Figure 1). This graphic 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 environment and requirements which must be met to achieve the desired evolution.

In the current state of communications, LMR networks and commercial broadband networks 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, the FirstNet Authority, in conjunction with public safety, is building out the NPSBN and public safety organizations will begin to transition to the FirstNet partner's public safety network from existing commercial broadband service. If and when the technical and non-technical requirements are met and are proven to achieve mission critical voice capability, it is anticipated agencies may 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 both 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 public safety responders with highly available, always on, reliable, and continuous connectivity between dispatch agencies and public safety users as well as among multiple agencies' users. Presently, dedicated LMR networks provide highly available voice services. The ability to talk user-to-user or one user to many while not connected to infrastructure is a critical feature.

Mission Critical Data

The public safety community uses wireless data communications to complement mission critical voice communications. Public safety currently uses wireless data services for many functions, such as dispatch; local, regional, state, and national and international license, vehicle, wanted person, criminal history database queries, messaging, and transmission of video and images. Public safety agencies have achieved wireless data capabilities by either building their own systems, subscribing to commercial wireless service providers, or combinations of both.

Although functional, many legacy LMR-based public safety wireless data services are generally limited in speed, coverage, and capacity and do not support advanced, real-time applications needed by public safety.

> Continuing to invest in the sustainment of current LMR networks and deployment of the NPSBN will need to be done simultaneously.

Nationwide Public Safety Broadband Network

Public safety envisions the NPSBN as a dedicated network built to public safety requirements using dedicated and allocated spectrum. With recent decisions by FirstNet regarding its commercial partner, agencies across the United States are considering whether to maintain their current contracts with other commercial services or to make the transition to FirstNet. As capability is built using LTE Advanced 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 continue using LTE for wireless data applications.

Commercial and Unlicensed Wireless Broadband Networks

The public safety community is increasing the use of commercial 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 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, critical broadband applications will be developed and deployed to the network as responders validate their capabilities.

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. FirstNet has developed a business plan which identifies, defines, and delineates the costs associated with the implementation and sustainment of the NPSBN as well as a user fee structure for subscribing agencies.

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, which was secured in spectrum auctions in 2015.

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 is collaborating with the Public Safety Communications Research lab and the National Institute of Standards and Technology to explore LTE services and the applications of LTE technology to public safety.

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 Federal, State, Local, Tribal, Territorial (F/S/L/T/T) levels, across jurisdictions and disciplines.

Planning: It is critical public safety stakeholders continually 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, which aligns and leverages existing governmental and commercial infrastructure and services. Further, the development of the NPSBN will require close coordination and partnering between the FirstNet Authority, its commercial partner, and the government. Public safety agencies need to evaluate their governance bodies to ensure they include those stakeholders who rely on and deliver communications during emergencies as well as communications 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. In the example of FirstNet, there is a nationwide governance structure which collaborates with F/S/L/T/T agencies to develop new initiatives, strategies, and timeframes related to investments and deployment of the NPSBN. The FirstNet Authority's Public Safety Advisory Committee assists FirstNet in carrying out its duties and responsibilities through the provision of subject matter expertise from representatives of the public safety community and its industry organizations.

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

RDT&E efforts will ensure emergency responders have reliable, effective, standardized, and interoperable wireless broadband capabilities and applications. Research and development is 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

CISA 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 stakeholders with the understanding that as the NPSBN evolves, the public safety 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:

Priority Access and Pre-Emption

Public safety 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 which 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 data is prioritized among various users and applications while ensuring reliable performance.

Reliability

For public safety 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 supporting public safety 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, public safety requires 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 to successfully accomplish their missions. In addition, FirstNet will be working to establish the best available wireless signal coverage to ensure reliable operations in wide geographic regions, including major population centers as well as rural areas.

Standards

Defining technical standards is critical to ensuring 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. Difficulties lie in public safety's ability to influence a global standard, such as LTE, because the public safety community represents a small percentage of the LTE consumer market. In addition to remaining aware and engaged with the 3rd Generation Partnership Project (3GPP) standards developments for LTE Advanced, the public safety community must also remain aware of continuing progress of Project 25 (P25) Telecommunications Industry Association (TIA) 102 LMR standards developments and revision. Primarily, the community should remain abreast of developments regarding LMR and LTE internetworking standards which will provide the physical and logical accredited technical standard(s) which will mirror 3GPPs efforts to provide mission critical push-to-talk services across the two technologies. Additionally, the community should reference the P25 Phase 2 standards, which provide for Console Subsystem Interface (CSSI) and Inter-RF subsystem Interface as these two standards define equipment and services, which can presently be used to connect an LMR system to an LTE network.

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. In the LTE Advanced standard, this is often referred to as Proximity Services (ProSe). It is an important capability 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 and 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 which may be outside of any LMR network coverage area, they may use direct mode to continue to communicate with each other despite reduced coverage.

Evolution of Mission Critical Voice and Data

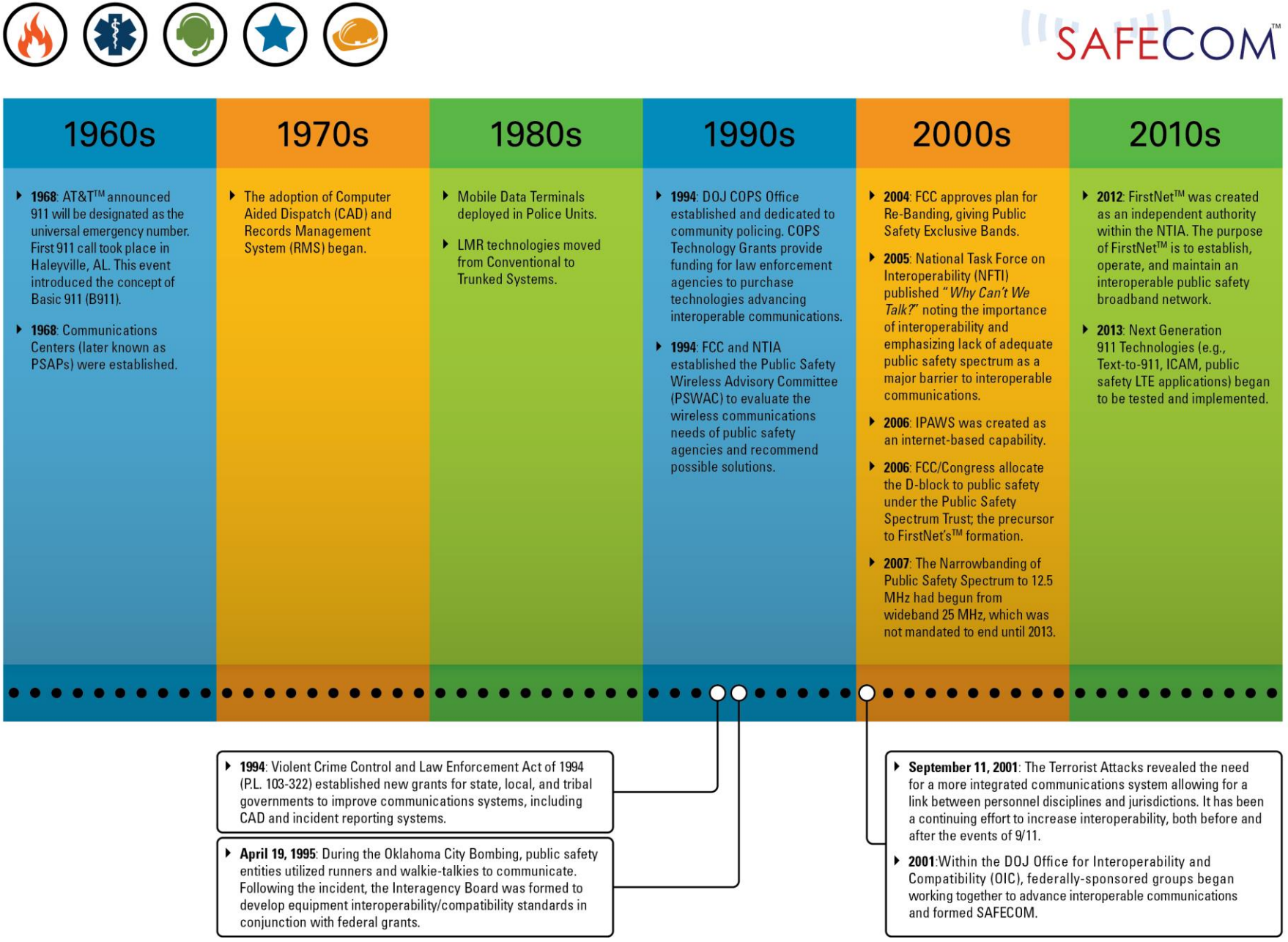
A "converged network" is a dedicated, public safety wireless broadband infrastructure capable of offering mission critical services, which include voice, data, and video, to public safety. It is important because it reduces the costs of developing and maintaining systems and increases the effectiveness of public safety in the field. However, convergence of LMR and LTE 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 the 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 timeframe for the availability of such technology.

It is necessary for public safety to continue investing in LMR in order to:

- Sustain existing systems
- Continue planning for new systems

<u>Appendix A</u>: Public Safety Communications Evolution Timeline

This appendix illustrates the technological advances, historical emergency incidents, legislative actions, and established committees which have contributed significantly to the evolution of public safety communications. Each milestone in the timeline, indicated by a black arrow, includes a description and the year it was enacted, occurred, or began. Milestones without a specific year attached to it are assumed to have occurred or were adopted over the decade to which it is assigned (by column). The black outlined boxes, located at the bottom of the graphic, represent specific noteworthy events and accomplishments.



Appendix B: Public Safety Communications Evolution Timeline - Continued

This appendix provides additional milestones not included in the *Timeline Graphic* in Appendix A. The rows highlighted in grey represent historical events while all other rows represent specific public safety communications technologies and efforts.

Date/Year/Decade	Description
1970	The use of **Telemetry Applications** by Emergency Medical Services from field to hospital was introduced.
1970s	Establishment of **Enhanced 911 (E911)** services including 911 selective routing, **Automatic Location Information (ALI)**, and **Automatic Number Identification (ANI)**.
1980s	**Cellular 1G Network** was developed and deployed.
January 13, 1982	The **Air Florida Flight 90 Crash** used Washington Area Fire Mutual Aid Radio System and Police Mutual Aid Radio System networks, Washington Area Warning Alert Systems were used but insufficient.
1989	**Project 25 (P25)** suite of digital standards for conventional and trunked public safety radio systems developed, promulgating a variety of requirements which enhance operations and interoperability.
1990s	**Cellular 2G Network** was developed and deployed.
1990s	**Geographic Information System (GIS)** began to be incorporated to support 911, CAD, RMS, and Tactical Mapping requirements in communications centers and PSAPs.
1996	Federal Communications Commission (FCC) issued the **Wireless Enhanced 911 Rules** to address the new technologies that had to be created in order to provide E911 services to all wireless callers. Implemented in two phases: • Phase 1: Within six months of a valid request by a PSAP, wireless carriers had to deliver the 911 caller's voice and originating cell site location to the most appropriate PSAP. • Phase 2: Phase II required wireless carriers, as of October 1, 2001 and within six months of a PSAP request for location information, to improve the location information used for call routing and caller location by providing the 911 system with the latitude and longitude of callers. Carriers were allowed to choose handset-based location technology using **Global Positioning Systems (GPS)**—or similar technology within individual wireless phones—or networked-based location technology using cell-tower triangulation.
1991	**Mobile Broadband/Data** was created. It allows wireless internet access through a portable modem.
1996	Nextel launches their **iDEN** (push-to-talk) network; a concept that would lay the foundation for mission-critical communications over cellular networks instead of the traditional LMR systems.
1997	**Emergency Alert System (EAS)** was created. This replaced the legacy EBS as noted for the Cuban Missile Crisis, moving from analog to digital alerting capabilities and Common Alerting Protocol.
1998	**Wireless Sensors** and **Machine-to-Machine (M2M)** capabilities (i.e., border control & security/central stations alarm systems) were implemented.

Date/Year/Decade	Description
1999	**Portable Fingerprint Scanners** were invented, primarily for Law Enforcement.
1999	**Public Safety Act of 1999** officially established 911 as the nation's emergency calling number.
2000s	**Cellular 3G Network** was developed and deployed.
2000s	**Cellular Data Networks** roll out vs. their traditional voice networks.
August 14, 2003	The **Northeast Blackout** was a reminder to have backup communications systems in place and has influenced continuity measures for emergency response personnel.
2005	The transition from **Public Switched Telephone Network (PSTN)** to **Internet Protocol (IP)** begins.
August 29, 2005	**Hurricane Katrina** saw the use of Public Safety Wireless Network Program audio matrix systems in Baton Rouge and New Orleans.
2006	**Inter RF Subsystem Interface (ISSI) Connectivity** was implemented.
2009	**Smart Building Systems** with on scene accountability tactical applications began to be developed and integrated to interact with jurisdictional CAD systems.
2010s	**Cellular 4G Network** was developed and deployed.
2010s	**Video** to include **Mobile and Airborne** uses with **Video Switching** (surveillance, video analytics) increasing over the decade.
2010s	**Augmented Intelligence Tools** starting to be developed and implemented.
April 20, 2010	The **Deepwater Horizon Oil Spill** led to the development of the **Gulf Coast Wireless Information Network (Gulf WIN)**, a 700/800 MHz interoperable radio network featuring fingertip roaming throughout the Gulf Coast region, this connected the U.S. Coast Guard with state and local responders.
April 15, 2013	During the **Boston Marathon Bombing,** public safety personnel maintained interoperable communications by using cache radios and building a super patch from six radio networks.
September 16, 2013	The **Washington Navy Yard Shooting** showed a use for social media during an incident. Multiple entities (the U.S. Navy, local public safety agencies, DC Mayor's office, etc.) used platforms such as Twitter and Facebook to provide updates on the evolving situation.