Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk

National Public Safety Telecommunications Council

Final Report

January 8, 2018

Table of Contents

Executive Summary 2

1. Introduction 9

1.1 Process 9

1.2 FirstNet Congressional Legislation 10

1.3 LMR Systems 10

1.4 LTE Push to Talk 11

1.5 LMR-LTE Integration and Interoperability 12

2. Existing Mission Critical Voice Reports & Activity 14

3. Open Standards Development Process 16

4. Examination of Public Safety Requirements 19

4.1 Use Case Overview 19

4.2 Additional Features 21

4.3 Public Safety Technical Requirements 21

5. Conclusions and Recommendations 43

APPENDIX A1: Public Safety Technical Requirements 49

APPENDIX A2: NPSTC PTT over LTE Report – 2013 53

APPENDIX A3: Public Safety Technical Requirements Analysis Chart 60

APPENDIX B: Public Safety Requirements Use Cases 75

APPENDIX C: NPSTC-PSCR Mission Critical Voice Round Table Report 103

APPENDIX D: 3GPP International Standards Information 110

APPENDIX E: Working Group Participant List 116

Executive Summary

Public safety Land Mobile Radio (LMR) systems provide mission critical communications for first responders and are considered essential to manage day-to-day agency operations and response to emergency incidents. The First Responder Network Authority (FirstNet) has estimated that there are more than 60,000 public safety agencies in the U.S. providing law enforcement, fire, and EMS services. All of these agencies are served by some form of public safety LMR system which includes Push to Talk (PTT) voice communications.

Some public safety agencies have implemented PTT services provided by commercial cellular providers, allowing them to shift administrative and support personnel to a non-mission critical communications system and lower operational costs. This service is called "Push to Talk over Cellular" or POC.[1]

The Nationwide Public Safety Broadband Network (NPSBN) being implemented by FirstNet will be the first fully interoperable network supporting data, voice, and video for all first responders in the U.S. The NPSBN is envisioned to transform public safety operations through the provision of new services, features, and capabilities. One of the proposed new services is Mission Critical Push to Talk (MCPTT), which is being designed to provide some LMR like services which may eventually allow first responders to carry a single device to access voice, video, and data. However, comparability with existing LMR systems for voice is yet to be determined, (e.g., for coverage and direct unit to unit communications).

This changing technology landscape may directly impact mission critical voice communications and the way that public safety agencies interoperate with each other and with other organizations and entities. A prioritized version of existing POC applications will increase its reliability and potentially accelerate its adoption by first responders. Standards to fully support MCPTT are still in development and the timeline for availability of the service is based on many factors and is unknown.

These developments mean that public safety agencies may be conducting some communications on both LMR and LTE networks. Adoption of these new technologies, like MCPTT, will occur only when public safety agencies have confidence that the systems will provide true mission critical functionality and local control as well as appropriate coverage and network capacity. As these systems are tested and put into use, public safety agencies will need a fully functional interworking[2] solution to support first responder communications. For example, a law enforcement officer using his/her LMR portable radio may need to communicate with a detective carrying an LTE handset. An incident commander at the scene of a major vehicle crash may need to communicate with first responders, telecommunicators, and support agencies using both LMR and LTE technologies.

[1] These PTT services may also be referred to as "Administrative Push to Talk" and "Cellular PTT."

[2] This report uses the 3GPP preferred nomenclature "Interworking" to indicate interoperability functionality is needed between LMR and LTE networks, as well as between one LTE network and another.

This report examines those operational considerations and identifies public safety technical requirements involving mission critical voice communications specifically targeting operational interoperability between LMR and LTE MCPTT. While the timeline for availability of MCPTT services is unknown, there are a number of issues that need to be addressed in the near term to better understand this service and to resolve specific technical issues that would impact first responders.

Mission Critical Voice also includes two-way simultaneous (duplex) voice[3] which will support hands free communications between first responders, dispatchers, and other entities as well as two-way video chat and telephony calling. Those elements of Mission Critical Voice only received a cursory examination in this report in order to maintain focus on LMR-LTE interoperability.

Forty-six public safety technical requirements were identified and grouped into one of eight categories:

1. Interoperability
2. Direct Mode
3. Talker ID
4. Emergency
5. Encryption
6. Scan
7. Full Duplex
8. LTE Consoles

Chapter 4 includes a complete listing of all requirements. Each section within that chapter contains a requirements chart (based on the eight categories listed above) and detailing public safety operational needs as well as providing background information to help clarify the intent and meaning of each item.

Chapter 5 of this report includes a series of conclusions and recommendations directly related to LMR-LTE integration. They include the following:

1. **Mission Critical Voice services are an essential element of the NPSBN.** The SAFECOM Interoperability Continuum should be used for guidance during all phases of implementation and on an ongoing basis. Beyond the Technology Lane (of the Continuum), attention must be paid to Training, Governance, SOPs, and Usage to ensure successful implementation of the NPSBN.

[3] Full duplex voice capability is also an important factor in allowing a Public Safety Telecommunicator in a PSAP or fixed dispatch center to override field unit voice transmissions in an emergency.

2. **Public safety agencies expect the NPSBN to support a robust multi-vendor ecosystem, and the availability of a wide range of user devices, equipment, and services using non-proprietary, open standards**. FirstNet must ensure that implementation of the NPSBN does not inadvertently create an unfair monopoly caused by the provision of equipment and services from a limited number of manufacturers. FirstNet should fully document their requirement for interoperability between and among devices and applications, including the use of Application Programming Interfaces (APIs) to help ensure that public safety agencies may select from a wide range of equipment offerings from different manufacturers.

3. **Integration of LMR and MCPTT services is required to support interoperability between first responders using both networks**. This interoperability requirement includes the need to pass PTT data between LMR and LTE systems to support the exchange of PTT ID and Emergency Alarm information. Standardization of this integration effort is critical to ensure common solutions are implemented nationwide. The Alliance for Telecommunication Solutions (ATIS) and the Telecommunications Industry Association (TIA) have created a Joint LMR/LTE (JLMRLTE) Subcommittee 8.8 to study requirements for interworking of LTE Mission Critical broadband services with existing Project 25 (P25) LMR systems. This work should be completed as soon as possible. Lack of a standard frequently results in the introduction of proprietary solutions which become imbedded in public safety operations.

4. **3GPP [3rd Generation Partnership] standards on direct mode PTT communications are not keeping pace with the deployment of MCPTT solutions.** In addition to accessing an LMR-LTE interoperability solution, first responders must have a robust local area off-network MCPTT communications capability that will allow uninterrupted service during a failure of network infrastructure or when a first responder transitions into an area without NPSBN coverage. In the absence of a standardized solution, vendors are introducing their own products that provide direct mode PTT voice. These solutions may not be interoperable with each other and may result in non-standards based solutions being introduced into the NPSBN. Public safety agencies should understand that some solutions may provide interim direct mode communications while standards work is completed. FirstNet should articulate a roadmap for direct mode voice communications and how early vendor-offered solutions will integrate with a future nationwide direct mode standard.

5. **Digital voice encryption is an important component for certain MCPTT communications on interworked LMR-LTE networks and must be considered when planning LMR-LTE integrated talkgroups**. There are many technical and policy issues surrounding encryption of LTE voice communications and encryption becomes more complicated when joint LMR-LTE talkgroups are involved and there is a need for “end-

to-end" encryption. FirstNet should provide information on how LMR and LTE encryption will be managed.

6. **Video chat function with full duplex voice is an important capability for first responders**. For example, this is an important function for EMS personnel who need to do a hands-free consultation with a medical control physician. Law enforcement and fire personnel will also make use of this function in a variety of settings. 3GPP work on Mission Critical Video should be monitored to help guide future implementation of these services**.**

7. **LTE consoles play an important role in the evolution of PTT and MCPTT services**. PSAPs and first responders may begin using POC to support administrative functions. This will require tight integration with existing LMR console equipment. The implementation of MCPTT will further require a purpose-built console device supporting a rich set of features and capabilities. Integration of LMR and LTE communications is essential, and some aspects of this function may be managed at the console level. Connection and interworking components to support LTE console functionality are not yet defined in 3GPP standards and additional first responder input is needed to help define needed capabilities for these devices. NPSTC produced an early report on LTE console functionality[4] that should be refreshed. FirstNet should advocate that 3GPP define a wireline dispatch interface for MCPTT if the evolving 3GPP interworking standard for LMR and LTE does not meet public safety's expectations. This same approach may be needed to obtain wireline interfaces to manage Mission Critical Data and Mission Critical Video.

During the development of this report, several key issues were identified that were outside the Working Group's focus on LMR-LTE interoperability. However, those issues are both important and indirectly impact LMR-LTE integration. They are noted in this report with a recommendation on follow up activities.

1. **Digital voice encryption is an important component for certain communications occurring exclusively on MCPTT talkgroups.** Certain technical, standards, and policy issues need further review and more information is needed on how encryption will be managed on the NPSBN and to what extent local public safety agencies will have control over management of encryption keys. Most public safety agencies tightly manage these resources and limit the sharing of encryption keys with other agencies. However, the NPSBN will allow nationwide MCPTT interoperability and thus introduce challenges with the effective implementation of encryption. NPSTC should task the LMR-LTE Integration and Interoperability Working Group to examine this issue and develop early

[4] See NPSTC LTE Console Report

recommendations for review and approval by the Governing Board and transmittal to the FirstNet Public Safety Advisory Committee (PSAC).

2. **Work is needed to assess technical and policy issues regarding the creation and management of MCPTT talkgroups**. As the Working Group was discussing the need to interconnect LMR and LTE talkgroups, it became apparent that the NPSBN will be supporting thousands of LTE talkgroups. Management of LTE talkgroups, including Talkgroup IDs and Talkgroup Aliases, is needed to prevent technical and operational challenges involving duplicate IDs and names. NPSTC should task the LMR-LTE Integration and Interoperability Working Group to examine this issue and develop early recommendations for review and approval by the Governing Board and transmittal to the PSAC.

3. **A nationwide standard is needed to define creation of PTT IDs by public safety agencies**. As the Working Group was discussing the need for MCPTT IDs to be exchanged with LMR PTT IDs, it became apparent that a standard will be needed to manage this information. This includes procedures for regionalization of nationwide LTE talkgroup coverage and the establishment of regional (state or multi-county) LTE interoperability talkgroup standards. FirstNet is providing a nationwide interoperable communications network that will allow first responder devices to operate virtually anywhere. The identity of the first responder is a critical safety feature and some form of identification is needed for itinerant users who have traveled outside of their home agency service area. NPSTC should task the LMR-LTE Integration and Interoperability Working Group to examine this issue and develop early recommendations for review and approval by the Governing Board and transmittal to the PSAC. FirstNet should also identify technical solutions for the provision of PTT ID, including whether Over-The-Air Alias (OTAA) is an appropriate solution.

4. **A standard is needed for nationwide LTE interoperability talkgroup names**. As the Working Group was discussing the operational aspects of LMR-LTE interoperability, it became aware of the need for standardized channel names for NPSBN talkgroup allocated for nationwide interoperability. LMR networks today support access to a set of FCC designated nationwide interoperability channels. These channels allow a first responder to communicate with local agencies while they are out of their home agency service area. Nationwide LMR interoperability channels have American National Standards Institute (ANSI)-standardized names to ensure that first responders from different agencies can locate the desired channel in their radio. A similar set of nationwide interoperable LTE talkgroups will be needed to mirror the existing LMR function. Those LTE talkgroups must have standardized channel names to create a common identity in all user devices. The NPSTC Governing Board recently authorized

the Common Channel Naming Working Group, which authored the ANSI standard for designated channel names for nationwide LMR channels, to start work on this project.

5. **MCPTT interoperability requirements must be considered**. As the Working Group was discussing LMR-LTE interoperability it became apparent that first responders will require the same level of interoperability when operating on different LTE networks. Public safety agencies require interoperability with other public safety agencies and responder organizations regardless of their network, technology, or spectrum band. Interoperability is as important between LMR and LTE as it is between different LTE networks. NPSTC recently completed a comprehensive report on the use of broadband deployable systems which was done as a cooperative effort with the Canadian government. A key take away from that report was the need for seamless interoperability between first responders on both sides of the international border. Public safety personnel need to access and share voice and data communications with other first responders operating at a common incident scene. That report concluded that an LTE core-to-core connection would likely be required between FirstNet and the Canadian Public Safety Broadband Network. This need for interoperability between first responders becomes more complex as additional commercial carriers begin to offer public safety broadband services on their networks. FirstNet should participate with the European Telecommunications Standards Institute (ETSI) program as they work to define a Compliance Assessment Program (CAP) to ensure interoperability between different devices and services provided by different manufacturers.

6. **Public safety agencies need to better understand how the NPSBN network will be operated and decisions on adoption of 3GPP standards.** There is uncertainty in how new releases of 3GPP standards will be implemented by manufacturers and network operators. For example, a 3GPP standard that describes the MCPTT Scan/Monitor function provides for simultaneous receipt of multiple audio streams to a user device. Some industry representatives have stated that LTE scan will be provided as a sequential monitor function – similar to how LMR scan works today. Another 3GPP standard allows first responder user devices, including those carried by field supervisors and Incident Commanders, to monitor direct mode communications simultaneously with network-based communications. Industry representatives have indicated that the requirement for a dual receiver will significantly change UE device hardware requirements and may not be commercially viable. Both FirstNet, and the public safety agencies it serves, need to understand the expected technical environment that will be supporting their operations. FirstNet should inform the PSAC on which public safety requirements noted in 3GPP standards will likely not be supported by the manufacturing community (e.g., chipset, device, and network operators).

7. **Public safety agencies should use caution when evaluating vendor equipment that is designated "mission critical.** Many vendors are using this phrase to market devices and solutions. This may make public safety agencies believe that the device or service is suitable for use by first responders in life and death situations. FirstNet should articulate how any given NPSBN product or service offering receives a "Public Safety Mission Critical" label, allowing first responders to know that a device/application/service has been independently evaluated and is suitable to perform in an emergency.

1. Introduction

Public safety LMR networks provide Mission Critical Push to Talk communications and are used by virtually every first responder in the U.S. The implementation of the NPSBN and the availability of MCPTT services will change the way public safety agencies operate and interoperate.

This report is designed to articulate the issues and requirements regarding integration and interoperability between LMR systems and LTE MCPTT services. This report does not advance a notion that all public safety agencies will migrate their LMR users to the NPSBN. However, it is clear that public safety agencies will be using a mix of LMR and LTE networks in both the short and long term and will need to have effective interoperability solutions.

NPSTC has addressed the issue of Mission Critical Voice in a number of prior reports, including a 2011 report *Mission Critical Voice Requirements for Public Safety* and a 2013 report *PTT over LTE for Public Safety*. NPSTC's prior work in this area, as well as reports from other organizations, is referenced in Chapter 2.

While this report frequently cites references to LMR Project 25 (P25) radio systems it must be noted that public safety agencies use a variety of other LMR networks. These include conventional repeaters and simplex channels across all frequency bands. These LMR systems must also be considered during the design of an LMR-LTE interoperability solution.

It is important to note that there are many technical and terminology differences between LMR and LTE systems. This report attempts to use standardized language wherever possible. For example, the term "talkgroup" has a very specific technical meaning in relation to an LMR trunked radio system and a very different technical meaning when used with LTE. While the phrase denotes the same functionality in each network the design, limitations, and capabilities of each system are different.

This report uses the acronym "NPSBN" to denote the Nationwide Public Safety Broadband Network, also known as FirstNet. Recently, additional LTE service providers have announced plans to offer public safety broadband services. The information, requirements, conclusions, and recommendations in this report are applicable to any provider that claims to offer services equivalent to those available on the NPSBN.

1.1 Process

NPSTC authorized the creation of an LMR-LTE Integration and Interoperability Working Group in 2016 to study how first responders would communicate with the introduction of MCPTT. More than 200 participants representing public safety, industry, and academia

participated on the Working Group and in the development of this report. Working Group members created use cases to examine different public safety operational scenarios involving the use of LMR and LTE PTT services. These use cases led to the creation of public safety technical requirements and a series of recommendations and conclusions. Consistent with NPSTC's transparency and review process, the Working Group's final report was then examined by a Public Safety Review Team consisting of first responders and other public safety agency personnel who were not involved in development of the document. The report was also distributed to the NPSTC Technology and Broadband Committee for review and comment. The updated document was then submitted to the sixteen member NPSTC Governing Board for review and approval. All NPSTC reports dealing with public safety broadband issues are then officially transmitted to the FirstNet Public Safety Advisory Committee (PSAC) for their consideration.

1.2 FIRSTNET CONGRESSIONAL LEGISLATION

FirstNet was created in 2012 via congressional legislation to build a Nationwide Public Safety Broadband Network. A major component of the NPSBN is to enable and support interoperability. Indeed, the genesis of FirstNet came from the 9/11 Commission Report which noted that a lack of voice interoperability disrupted emergency operations and was life threatening for first responders. In order to fully support first responder interoperability, Congress required that FirstNet build the network using open, non-proprietary standards.[5] The adoption of open standards is an essential component to meet the need for interoperability between LMR and LTE networks and is necessary to adopt the requirements and recommendations contained in this report.

1.3 LMR SYSTEMS

Public safety agencies rely on Mission Critical Voice communications to conduct daily operations and to manage complex emergency events. Public safety LMR systems are purposely built and designed to support individual and group communications. These systems are typically voice centric and operate as a self-contained local network. Public safety LMR systems also provide crucial off network service allowing direct communications between first responders without the need for infrastructure.

There are a wide range of LMR systems in use by public safety agencies today. These include analog and digital systems, networks that use simplex channels, conventional repeaters, and trunking radio technology. Three forms of LMR have defined standards in North America. They include P25 Trunking, P25 Conventional, and Analog. Some systems are built using proprietary digital solutions offered by a specific manufacturer. The type of system built by a public safety agency is based on a number of factors including cost, coverage, features, and need for interoperability. Public safety LMR networks operate in many frequency bands including VHF, UHF, 700 MHz, and 800 MHz. Additionally, public

[5] Section 6206(b)(2), establishes a requirement that FirstNet promote competition in the equipment market, (i) that equipment be built to open, non-proprietary, commercially available standards; (ii) capable of being used by any public safety entity and by multiple vendors.

safety agencies use a variety of console and gateway systems to operate and manage their LMR networks.

This use of disparate spectrum and different technology creates interoperability challenges. The adoption of the P25 digital radio standard has greatly enhanced the interoperability landscape. There are a number of solutions[6] in use today to create interoperability between public safety LMR systems. These include simple console patching and the use of IP gateways as well as other mechanisms to support local needs. Some of these interoperability solutions will likely be leveraged to support LMR-LTE interoperability.

1.4 LTE PUSH TO TALK

LTE networks are multipurpose and data centric. They are capable of supporting different types of voice, data, and video services. This includes full-duplex voice communication (e.g., telephony and video chat) as well as PTT voice. Commercial cellular companies provide Push to Talk via POC applications which may be designed for different user groups and are typically divided into two categories, PTT and Mission Critical PTT (MCPTT). While MCPTT is based on 3GPP international standards that are continuing to evolve, several vendors offer POC solutions today. These may be implemented as either a network service or an Over-The-Top application. While true Mission Critical PTT is not available today, some agencies are using existing POC solutions during incident response and in mission critical environments.

Just as interoperability between LMR and MCPTT is essential, so is interoperability between first responders who may be using different POC services. While there is a clear expectation that all first responders using MCPTT will be able to interoperate, this is less clear when discussing the use of different PTT solutions. A police officer using POC Solution "A" must be able to communicate with a sheriff's deputy using POC Solution "B."

Direct mode PTT communications in LTE, which are conducted without any cellular infrastructure support, are also essential for public safety agencies and are a key safety component to protect first responders. However, LTE direct mode communications are still under development by 3GPP. Work is continuing on an LTE direct mode solution for public safety called "ProSe" (named for Proximity based Services). This is designed to support direct user to user voice, data, and video communications. In the meantime, industry is introducing alternative solutions in some public safety handsets including dual-mode user devices which support both LMR and on-network LTE communications and the provision of a narrowband voice radio within the LTE handset to provide direct mode capabilities. The introduction of various interim direct mode solutions may negatively impact long term interoperability. Public safety agencies will need a common LTE direct mode solution to achieve interoperable communications.

[6] These include the Inter Sub-System Interface (ISSI), the Console Sub-System Interface (CSSI), the Bridging Systems Interface (BSI) as well as Radio Over IP (ROIP), conventional console patching and other IP gateway solutions.

1.5 LMR-LTE INTEGRATION AND INTEROPERABILITY

The need for effective interoperability between LMR and LTE networks is now of paramount importance. Public safety agencies are likely to embrace the availability of existing POC solutions. These POC applications will receive priority on the NPSBN[7] making them more reliable. In 2018, first responders will also have preemption capabilities which will further increase the reliability of these POC solutions.

There are a variety of operational considerations and migration options that should be considered when contemplating the design of LMR-LTE interoperability.

- Interoperability may be needed within an agency to support the use of both LMR and LTE services which are assigned to different employees based on their agency role.
- Interoperability may be needed within an agency as it transitions all of their users from LMR to LTE.
- Interoperability may be needed by an agency to support interoperable communications with another agency on a disparate system (LMR or LTE).

This report concluded that LMR and LTE interoperability will be required over an extended period of time. It is likely that some public safety agencies may never migrate their LMR operations over to LTE. First responders will also continue to need interoperability with other government and private entities which will remain on LMR networks.

Public safety agencies should reference the SAFECOM Interoperability Continuum to assess all of the factors needed to achieve successful interoperability with LTE. While the Continuum was designed around LMR interoperability, the five “travel” lanes are also applicable to LMR-LTE interoperability.

This report does not prescribe an LMR-LTE interworking solution. The Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) have created a Joint LMR/LTE (JLMRLTE) Subcommittee 8.8 to study requirements for interworking of LTE Mission Critical broadband services with existing P25 LMR systems. While there are existing LMR-LTE interfaces in use today by public safety agencies, it is important that the standardized solution include all of the requirements necessary for effective interoperability. LMR-LTE interoperability must include more than the exchange of voice traffic. This report articulates the need for the exchange of various data elements, including PTT ID, Emergency Alert, and location information. Digital encryption is used by many public safety agencies today on their LMR networks and first responders will need a solution that supports end-to-end encryption during joint

[7] AT&T and Verizon have both indicated that they will prioritize public safety traffic on their traditional LTE networks as well.

operations, where agency personnel are using both LMR and LTE interconnected talkgroups.

As noted earlier in this report, some solutions designed for LMR system interoperability may be leveraged to provide LMR-LTE interoperability. Finally, it should be recognized that public safety agencies come in all sizes and configurations. Many agencies face budgetary constraints and will not be able to afford feature-rich interoperability solutions. This requires the availability of a range of interworking solutions which will meet the requirements of small agencies with basic needs as well as large agencies using complex systems.

2. Existing Mission Critical Voice Reports & Activity

NPSTC has produced a number of reports that articulate functionality needed by first responders using the NPSBN. Many of these reports deal with Mission Critical Voice (MCV) including specific recommendations for MCPTT services. In addition, NPSTC has participated in a number of working group sessions sponsored by the Public Safety Communications Research (PSCR) program within the U.S. Department of Commerce. The associated public safety technical requirements listed in the following reports and documents should be considered complimentary to the recommendations made in this document.

- **Mission Critical Voice Communications Requirements for Public Safety.**[8] This report, published in 2011, provided early technical requirements in seven areas: Direct Mode/Talk Around, Push to Talk, Full Duplex Voice Systems, Group Call, Talker Identification, Emergency Alerting, and Audio Quality.

- **Public Safety Broadband, Push to Talk over Long Term Evolution (LTE) Requirements.**[9]This report, published in 2013, articulated a shared vision for Public Safety Grade communications, Reliability, and Resiliency. It also described the need for an LTE interface to public safety LMR systems as well as further defining the need for off network direct mode communications.

- **Public Safety Broadband Console Requirements.**[10] This report, published in September of 2012, identified 54 technical requirements around needed functionality for console systems that would support first responders. The requirements were allocated into seven categories: Network, Data Management, Location, Messaging, Priority, Security, and User Equipment.

- **Public Safety Communications Research (PSCR) Round Table Discussion on Floor Control and Direct Mode.** A series of conference calls were held between July and October of 2016 to discuss operational issues and requirements for public safety agencies as they program and manage their P25 radio networks. Specifically, the issue of prioritization of talkgroup access was reviewed, in the context of how these

[8] Report available on NPSTC website: http://npstc.org/download.jsp?tableId=37&column=217&id=2055&file=Mission%20Critical%20Voice%20Functional%20Description%20083011.pdf

[9] Report available on NPSTC website: http://npstc.org/download.jsp?tableId=37&column=217&id=2813&file=PTT_Over_LTE_Master_130719.pdf

[10] Report available on NPSTC website: http://npstc.org/download.jsp?tableId=37&column=217&id=3205&file=Console_LTE_Report_FINAL_20140930.pdf

services may be provisioned in an LTE environment. A separate discussion was launched to examine operational implications with direct mode voice communications in LTE networks. This information is included as Appendix C.

- **PSCR Round Table Meeting on MCV Key Performance Indicators.**[11] This meeting was held on March 9, 2017, in Boulder, Colorado, and sponsored by PSCR. This session focused on key performance indicators that would measure a successful Mission Critical Voice implementation. It also introduced a "Quality of Experience" or QoE metric. Participants matched each QoE area with testing metrics used to evaluate elements of voice communication technology. Eight QoE areas emerged as most important for benchmarking public safety MCV, and a test framework was developed for each. The eight QoE areas are:
    1. Access to Communications
    2. Audio Quality
    3. Context/Situational Awareness
    4. Coverage
    5. Interoperability
    6. Priority
    7. Security
    8. Usability

It should be noted that PSCR has funded several innovation grants that deal with Mission Critical Voice communications, including LMR-LTE interoperability.[12] Final reports from these initiatives should be available in 2018 and 2019.

[11] The full report is available at this link: http://npstc.org/download.jsp?tableId=37&column=217&id=4003&file=NPSTC_PSCR_MCV_Summary_Appendix_Full_Doc_161111.pdf

[12] The full list of PSCR grants is available here: https://www.nist.gov/ctl/pscr/funding-partnerships/grants/psiap-awardees

3. Open Standards Development Process

The importance of standards to support the NPSBN cannot be overstated. The congressional law authorizing FirstNet requires the use of nonproprietary open standards.[13] In addition to network design, standards are an essential component to support interoperability. This action was designed to ensure that first responders would be able to communicate with each other in an emergency. FirstNet noted the importance of standards in their RFP documents which required offerors to use standards-based, nonproprietary solutions.

It is also important to note FirstNet's obligations in the standards development process. Section 6206 of the law that created the First Responder Network Authority states that FirstNet is responsible to engage in any standards proceeding that deals with interoperability:

> SEC. 6206. POWERS, DUTIES, AND RESPONSIBILITIES OF THE FIRST RESPONDER NETWORK AUTHORITY.
> (c) OTHER SPECIFIC DUTIES AND RESPONSIBILITIES.
> (7) REPRESENTATION BEFORE STANDARD SETTING ENTITIES.
>
> The First Responder Network Authority, in consultation with the Director of NIST, the Commission, and the public safety advisory committee established under section 6205(a), shall represent the interests of public safety users of the nationwide public safety broadband network before any proceeding, negotiation, or other matter in which a standards organization, standards body, standards development organization, or any other recognized standards-setting entity addresses the development of standards relating to interoperability.

There are two main Standards Development Organizations (SDOs) that manage issues involving the NPSBN and LMR-LTE Interoperability. They are the 3rd Generation Partnership Project (3GPP) and TIA.

3GPP is a global standards development organization that focuses on commercial cellular operations, including Long Term Evolution (LTE). Work is ongoing in 3GPP to develop new standards and to enhance existing standards involving mission critical services. Activity in 3GPP Release 15 is currently focused on the creation of an LMR-LTE interface. These standards will define which features and capabilities of LTE MCPTT will be supported via an interconnection with LMR. 3GPP Release 15, Stage 2 work includes the design of an Inter-Working Function (IWF) that will allow LMR and LTE services to interoperate. As of the date of this report, 3GPP plans to have their Release 15, Stage 2 LMR-LTE interworking design work done by the end of

[13] Section 6206(b)(2) of the law indicates that the prime objective of this clause is to promote competition.

2017, and Release 15, Stage 3 work done in the June 2018 timeframe. The 3GPP SA6 group has created a significant body of work as of the date of this report.

ATIS and TIA have created a Joint LMR/LTE (JLMRLTE) Subcommittee 8.8 to study requirements for interworking of LTE Mission Critical broadband services with existing P25 LMR systems. This effort has been put on hold pending advancement of the 3GPP Mission Critical services architecture referenced above. As of the date of this report, both ATIS and TIA TR-8.8 expect this work to be restarted in late 2017 or early 2018. That work is expected to produce a study of the common services that are candidates for MC LTE interworking with P25 LMR and a high level overview of the technical challenges associated with interworking of those services. This study will enable a more informed view of what additional interworking standards may be needed and whether ATIS or TIA will produce and maintain such standards. Note that a similar study has been published by ETSI that provides this same level of information in the context of MC LTE and TETRA interworking.

Interoperability between public safety LMR systems was extremely difficult prior to the adoption of the P25 radio standard. Work efforts within 3GPP and TIA must remain a high priority in order to finalize an industry standard for LMR-LTE interoperability and interworking. It is important to acknowledge that the presence of a standard does not always translate into service capability. Following the completion of an industry standard, network operators may or may not elect to adopt them; industry may, or may not, elect to include the features and capabilities in future chipsets and user equipment; and vendors may continue to design features and capabilities that are different than the standard. For example, a 3GPP standard describes an MCPTT feature that allows a first responder to monitor multiple talkgroup audio streams simultaneously. This was viewed as an enhanced scan capability that is not possible on LMR systems. Industry has indicated that they plan to implement an LTE scan solution using delivery of single sequential talkgroup audio.

In some cases, standards may be implemented by vendors in different ways resulting in non-compatible equipment. These issues were evident with early implementation of the P25 standard which was designed to allow subscriber equipment from any manufacturer to operate and interoperate with other P25 vendor equipment. It was determined that while both vendors built subscriber devices using the P25 standard, a P25 radio from Vendor A would not work on Vendor B's P25 network. These issues led to the creation of a P25 Compliance Assessment Program which sought to provide testing and certification that vendor equipment would interoperate. Today, the number of interoperability issues between P25 manufacturers is low.

The European Telecommunications Standards Institute (ETSI) has recognized this issue and is working to develop a Compliance Assessment Program that will ensure operability and interoperability between different LTE device manufacturers providing MCPTT service.

Public safety agencies should continue to monitor the work of 3GPP and TIA as these standards evolve. Input from first responders and from FirstNet will be essential in order to articulate needed functionality. Manufactures of P25 systems should be encouraged to adopt updated 'core' LMR-LTE standards as a part of P25 LMR system updates.

4. Examination of Public Safety Requirements

This chapter conducts an examination of existing public safety technical requirements involving Mission Critical Voice communications, including those specifically targeting operational interoperability between LMR and MCPTT. It should be noted that Mission Critical Voice also includes two-way simultaneous (duplex) voice[14] which will support hands free communications between first responders, dispatchers, and other entities as well as two-way video chat and telephony calling. Those elements of Mission Critical Voice received a cursory examination in order to maintain the focus of the report on LMR-LTE interoperability.

Information was also obtained from several other NPSTC documents identified in Chapter 2 of this report. Additionally, eight use cases were developed to assess public safety's use of mission critical voice in a variety of scenarios. Interoperability features to support first responders using both LMR and LTE networks were assessed against existing features and capabilities available in P25 digital LMR systems. While the P25 standard was used as a baseline, it is recognized that public safety agencies also operate on conventional radio networks using analog and non-P25 digital technologies. To the extent practical, consideration was given to support interoperability between LTE Mission Critical Voice services and these other networks.

A series of public safety technical requirements were identified across the eight use cases. These were consolidated to eliminate duplicates and to extract only those technical requirements applicable for this report. The remaining requirements were then rated to determine which ones should be declared mandatory and which ones would be assigned as optional.

4.1 Use Case Overview

The eight use cases created for this report were designed to illustrate emergency response events that occur on an everyday basis. This report did not examine the unique interoperability requirements that would exist at a major incident or disaster scene.

Use Case 1: Single Talkgroup PTT Voice Interworking: This use case examined the basic concept of LMR and LTE interoperability during the response to a burglary alarm at a jewelry store. Officers using LTE Mission Critical Voice needed assistance from a Sheriff's Office canine unit which was operating on an LMR radio network.

[14] Full duplex voice capability is also an important factor in allowing a Public Safety Telecommunicator in a PSAP of fixed dispatch facility to override field unit voice transmissions in an emergency. Full duplex voice is also an important component in certain LTE applications which will allow first responders to access "hands free" communications.

Use Case 2: Multiple interconnected LMR/LTE talkgroups. This use case examined LMR-LTE interoperability at the scene of an apartment complex fire involving law enforcement, fire, and EMS units. The primary responding agency was operating on LTE but mutual aid fire and EMS personnel were using LMR. Multiple interconnected talkgroups were needed to support on scene incident communications.

Use Case 3: Off Network Communications. This use case examined off network communications at the scene of a construction accident involving an injured worker at the base of an elevator shaft. First responders were using both LTE and LMR radio networks. Personnel treating the patient were in a sub-basement with no network coverage and were using direct mode communications. This use case identified the need for first responders using LTE direct mode to communicate with other first responders using LMR direct mode. While it is not technically possible for an LTE device to communicate directly to an LMR device, the operational requirement is still valid and will require some type of assistive technology to support the needed capability.

Use Case 4: Consultation/Full Duplex Voice. This use case examined the need for "hands free" full duplex voice communication at the scene of an incident in which a paramedic required video consultation with a physician in the Trauma Center. Discussion on the need for full duplex voice communications then extended to include the need to support PSTN telephone calls, conversational voice between first responders, and full duplex to support console audio override.

Use Case 5: Incident Command Scan. This use case examined the need for first responders to scan multiple talkgroups to maintain situational awareness at the scene of an incident. Existing scan features available in P25 radios were benchmarked against LTE Mission Critical Voice. The LTE network will need to support scanning that includes LMR-LTE interworked talkgroups. While 3GPP standards provide for the simultaneous delivery of multiple audio streams to a first responder's device, many public safety agencies have indicated that they prefer the LTE radio to provide sequential scan audio. This would more closely align the scan function of the two networks. It was also noted that LMR networks will need to support sequential scan audio feeds coming from interworked LTE talkgroups.

Use Case 6: LTE Talker ID and LTE Emergency Call Button. This use case examined the role of LTE Talker ID, LTE Talker Alias, and the activation of the Emergency Call Button during incidents involving first responders operating on interworked LMR and LTE networks. This is a complex area of study that yielded a number of policy and governance issues beyond the technical requirements identified to support on scene operations.

Use Case 7: Cellular Push to Talk/Over the Top Push to Talk. This use case examined the need for first responders to interoperate with other external networks, beyond the LMR and LTE mission critical voice systems. In the case study, public safety personnel working at a county fair need to communicate with personnel using a Push to Talk voice application operating on a commercial cellular network.

Use Case 8: Encryption. This use case examined the need for first responders to conduct secure voice and data communications and builds on Use Case #1 involving response to the burglary alarm at the jewelry store. Public safety personnel will need to use encryption in a variety of scenarios, including during joint operations involving personnel using both LMR and LTE voice networks.

4.2 Additional Features

The Working Group also examined a number of other features supported on P25 networks and noted that parity with existing LMR capabilities would likely be expected by public safety agencies. These include:

1. Listen Only feature
2. Individual Calls [one-to-one]
3. Emergency Alert
4. Radio Check
5. Call Alert
6. Radio Monitor
7. Radio Inhibit/Uninhibit/Status
8. Location Services
9. Text/Short Message Service
10. Talker Override/Floor Control
11. Late Entry of Audio
12. Regrouping (relating to encryption and tactical reorganization)

4.3 Public Safety Technical Requirements

Information from each of the use cases generated additional discussion which resulted in the creation of 46 public safety technical requirements. These requirements were grouped into one of eight categories:

1. Interoperability
2. Direct Mode
3. Talker ID
4. Emergency
5. Encryption
6. Scan

7. Full Duplex
8. LTE Consoles

The following information provides background into each of the categories and also identifies the public safety technical requirements for that section. It should be noted that the Working Group also identified requirements that indirectly deal with LMR-LTE Interoperability. These are flagged with an asterisk (*) and have explanatory information included in Chapter 5.

4.3.1 INTEROPERABILITY

At the core of this report is the need for first responders operating on LMR and LTE networks to communicate with each other. This need for two-way PTT communications exists across all daily operations and emergency response conditions. Public safety personnel need to communicate with each other while responding to an incident, while on the scene of an incident, and while operating inside buildings and structures that impact network coverage.

The use of interworked LMR and LTE talkgroups would support this interoperability requirement. These talkgroups could be created in advance and provide ongoing interoperability or they could be created on an ad hoc basis to connect specific LMR and LTE talkgroups used by first responders during an incident.

It is important to note that telecommunicators in the Public Safety Answering Point (PSAP) also need these interoperability capabilities and must be able to communicate with first responders operating on both networks. This need is reflected by the requirements in Section 6202(b)(2)(B)(ii) of The Act which requires FirstNet to integrate with PSAP systems. NPSTC has also published a report on Public Safety LTE Consoles which details a number of requirements for PSAP LTE equipment.

Larger scale incidents may involve many public safety agencies and disciplines (e.g., law enforcement, fire, and EMS) which would need access to multiple interworked LMR-LTE talkgroups to support operations. Law enforcement, fire, and EMS agencies may each need several talkgroups to coordinate their respective efforts, plus additional talkgroups for collaboration and control.

Related to this discussion is the issue of how LTE talkgroups are created. A standardized process must be used to ensure that duplicate talkgroup IDs are not assigned. The naming convention and alphanumeric “bit” sequence used for LTE talkgroup IDs should be explored to determine if a specific character sequence would be beneficial to support the interconnection of LMR-LTE talkgroups. The use of LTE talkgroup aliases should also be explored.

Based on the information contained in this chapter, the following public safety technical requirements were identified. *Note: The Working Group also identified requirements that indirectly deal with LMR-LTE Interoperability. These are flagged with an asterisk (*) and have explanatory information included in Chapter 5.*

#	Requirements
1	First responders operating on LMR and LTE networks SHALL be able to communicate with each other while responding to the scene of the incident as well as upon arrival.
2	Consoles operating on LMR and LTE networks SHALL be able to monitor and participate in the voice communications on interworked LMR and LTE talkgroups.
3	First responders and consoles SHALL have access to multiple LTE talkgroups to coordinate on scene operations and many of these LTE talkgroups will need to be interconnected with LMR talkgroups to support incident operations.

4.3.2 DIRECT MODE

In many cases, the safety of first responder personnel is based on immediate access to reliable voice communications. Two-way communications must be provided in all operational environments, including in locations where network coverage may be hampered or nonexistent.[15]

LMR systems used by first responders support both network assisted communication (e.g., communications through a repeater or trunked radio system) as well as simplex communications directly between two radio devices. A number of nationally recognized standards organizations, including the National Fire Protection Association (NFPA), require that public safety personnel have ready access to direct mode communications.[16]

LTE communications have historically been networked and recent efforts by 3GPP have identified a framework for LTE direct mode operations, called "ProSe." A number of standards have been identified in ProSe to mirror similar capabilities found in LMR networks. This work is

[15] It is recognized that there are areas in most jurisdictions where LMR radio networks do not provide coverage. First responders must be able to switch to a radio channel that allows direct mode communications which do not rely on radio system infrastructure.

[16] NFPA Standard 1221, Section 8.3.1.3 regarding availability of simplex radio communications capability at the scene of an emergency incident.

ongoing and will be enhanced in future 3GPP Releases.[17] It should also be noted that the output power on an LMR channel is significantly stronger than the allowable output power on an LTE device. This will impact the effective range of an LTE device operating in direct mode.

Other LTE technologies are also being investigated to support first responders, including the Vehicle to Vehicle (V2V) standard used to provide an off network, direct data exchange between cars, trucks, and other vehicles as part of the Intelligent Transportation System (ITS) initiative. This report identifies requirements necessary to support first responders in all operational environments, including groups of users who may be operating either on or off the network at the same incident.

The Working Group identified several important elements of direct mode communications that resulted in new technical requirements. These new requirements should be viewed as complementary to previously identified requirements for Mission Critical Voice.

In today's LMR environment, first responders manually switch their radio to "toggle" between network assisted communications (e.g., trunked or repeated systems) and simplex communications (e.g., direct mode voice). Some LMR radio systems provide a warning tone alerting the first responder that they are losing network connectivity, while in other cases, the first responder assesses the quality of the received audio to determine that they are likely out of network coverage.

The 3GPP standard for ProSe communications provides that an LTE device will automatically switch to direct mode communications when it senses a loss of network coverage. The Working Group identified a number of concerns with this approach, including problems in determining which threshold setting should be used to force an LTE radio to direct mode. Cover in buildings may be intermittent as a first responder moves through the structure and their radio may be "out" and "in" coverage repeatedly every few feet. This could result in the LTE radio automatically leaving the macro network and switching to direct mode and back continuously. The preferred mode of operation is for this feature to be managed by the local public safety agency, which may enable an automatic switch or enable a warning tone without an automatic switch, or may disable the automatic switch feature entirely.

The second concern regarding an automatic switch from macro coverage to direct mode involves the decision of which direct mode LTE Talkgroup the radio will select. Local public safety agencies may have different needs based on their size and operating environment. For example, if a police officer is inside a building during a high risk incident and loses connectivity with the radio network, should his radio switch to:

[17] The current version of this 3GPP standard 23.303 can be found here: http://www.3gpp.org/ftp//Specs/archive/23_series/23.303/

- A direct mode LTE talkgroup used by that police department.
- A common interoperable LTE direct mode talkgroup accessible to public safety.
- A common interoperable LTE direct mode talkgroup accessible to all FirstNet authorized devices, including Extended Public Safety users.

Depending on the circumstances, the officer may need assistance from anyone who is in radio range of their device, even if that person is a utilities supervisor. However, during a high risk warrant service, officers are working in a group and use of a dedicated LTE talkgroup for that agency may be the best approach. The local public safety agency should determine which default direct mode talkgroup would be selected by the device. While a first responder would be able to manually select other direct mode LTE talkgroups, in some emergency situations they would not be physically able to adjust their radio.

Public safety personnel may desire to work on LTE direct mode talkgroups even while in the coverage footprint of the LTE macro network. During a major incident, there may be multiple groups of first responders working in teams to accomplish specific missions. These groups may be assigned to LTE direct mode talkgroups to achieve better use of spectral resources. Direct mode RF signals travel short distances and direct mode radio frequencies can be reused with an appropriate geographical separation. In other cases, radio coverage may be intermittent inside a building or following damage to NPSBN infrastructure. In these situations, an Incident Commander may instruct personnel to operate on LTE direct mode to have assured communications. First responders would need to "force" their radio to remain in direct mode even though their device has sensed the presence of macro coverage and is trying to automatically move them back onto the network.

At an incident scene, it is not unusual for groups of first responders to be operating on LMR direct mode while other groups of first responders are operating on LMR trunked or repeated infrastructure. In most cases,[18] Incident Commanders and field supervisors must carry two radio devices in order to communicate with all of the first responders. With the emergence of new LTE technology, the preferred method of operation would be for LTE devices to have two receivers allowing an incident commander to simultaneously receive radio traffic from first responders on either the macro network or on direct mode. This need to monitor the direct mode talkgroup for radio traffic has significant safety implications for all first responders. For example, two police officers are inside a building searching for a burglary suspect and one of the officers enters a basement area and loses connection to the macro network. That officer's radio may automatically switch to an LTE direct mode talkgroup or the officer may manually select a direct mode LTE talkgroup. Once the officer has switched to direct mode, who do they communicate with? No other LTE device in the area is on that LTE direct mode talkgroup. With

[18] If an agency is using a conventional repeater, it is possible (based on frequency planning) for a single radio to receive both repeater and direct communications.

a single receiver, the other officer's radio is only able to receive transmissions from the macro network LTE talkgroup. That officer will be unaware that his partner is "off network" and in need of assistance.

The aforementioned scenarios also illustrate why it is important that Primary Public Safety and Extended Primary Public Safety users all have access to direct mode communications. Extended Primary Public Safety users may be at the incident scene and working to assist the Primary Public Safety agencies and therefore may need to communicate and coordinate their operations. This type of local government assistance is supported on many public safety LMR networks today, in which law enforcement, fire, and EMS agencies may communicate directly with public works, transportation, and utilities representatives.

There is also a need to support an emergency broadcast to all devices operating in a specific geographic area. During a building fire, hazardous materials incident, or active shooter response, an Incident Commander may need to order all personnel to leave the building immediately or direct them to take other actions. These emergency messages must be broadcast on the macro network LTE talkgroups (initiated by the PSAP or an Incident Commander) and functionality must exist to transmit emergency messages to users who are on direct mode LTE talkgroups (initiated by an Incident Commander at the scene). While it is possible to transmit an emergency message to all users on a specific LTE talkgroup, users may be operating on a more than a dozen separate LTE talkgroups. A capability is needed that would allow an emergency broadcast to reach all devices within a specific geographic area, regardless of which LTE talkgroup they were using. This type of network broadcast is similar to how Wireless Emergency Alerts (WEA) may be used to alert the cell phones of citizens associated to a particular tower site (or tower face). These alerts must reach all FirstNet authorized devices, including Primary Public Safety and Extended Primary Public Safety categories. While most alerts may be launched from an LTE console in the PSAP, it may be necessary for an alert to be launched from an authorized user device in order to reach those users operating on direct mode outside of the macro coverage.

Based on the information contained in this chapter, the following public safety technical requirements were identified.

#	Requirements
4*	Local configuration settings SHALL determine the user device's response when it identifies a loss of macro network coverage. The device may be programmed to automatically switch to an agency specified direct mode talkgroup or require that the device be manually switched to direct mode.

5*	Local configuration settings SHALL determine which direct mode LTE talkgroup the user's device switches to when it senses a loss of macro network coverage (e.g., does the device switch to a common interoperable LTE talkgroup or a discipline or agency specific LTE talkgroup).
6*	A first responder SHALL be able to manually set their LTE device to remain in a specific mode of operation regardless of the presence or absence of macro network coverage. This includes setting the device to remain on the macro network or setting the device to remain in direct mode.
7*	A first responder SHALL be able to communicate with personnel who are on either the macro network or operating in direct mode.[19]
8*	First Responders (e.g., Primary Public Safety users) SHALL be able to communicate with Extended Primary Public Safety users using direct mode (e.g., mass transit supervisor, DOT snow plow, utility worker).
9*	A direct mode emergency broadcast message SHALL reach all devices on all LTE direct mode talkgroups within RF range, including Primary and Extended Primary Public Safety users.
10*	An emergency broadcast message SHALL reach all FirstNet devices in the immediate area on all macro LTE talkgroups providing an alert to both Primary and Extended Public Safety users.

4.3.3 TALKER ID

Talker ID, also known as "Unit ID," "Push to Talk ID," and "PTT ID," is considered a key safety feature by public safety agencies. Telecommunicators in PSAPs and first responders in the field, can determine which unit is talking or attempting to transmit. There are frequent situations where immediate assistance is needed but the call for help is not intelligible due to background noise (e.g., a struggle with a suspect) or because the radio is in a poor coverage area. Talker ID data allows for the rapid identification of first responders who are in distress and also provides key operational information to Incident Commanders and telecommunicators.

Management of Talker ID data is a complex process that requires deliberate action by public safety agencies. Public safety radios are seldom used in a fixed assignment and portable radios may be shared between multiple personnel. For example, a set of portable radios may be

[19] It is recognized that communications in direct mode are range limited. 3GPP provides for a device with a dual receiver, where an Incident Commander at a scene could communicate with the dispatcher using LTE network and also with a nearby first responder who is on direct mode operating inside the building.

shared by firefighters on an engine company from shift to shift. A police officer may check out a portable radio for use on their shift and that same radio may be used by a patrol supervisor working the following shift.

While mobile radios are typically assigned to the specific vehicles they are installed in, their "inventory locations" may change. Mobile radios in police cars and fire trucks may be swapped out by support personnel for needed maintenance and repair. Portable radios may be permanently assigned to specific supervisory and command personnel, but may be loaned to other first responders. Some radios are assigned to a function (e.g., Engine 31 company officer) while others are assigned to a specific individual (e.g., a radio assigned to Officer James Taylor).

Depending on how LMR radio systems in a given region are organized, a first responder's radio may contain multiple Talker IDs based on the number of radio personalities (or separate radio systems) that the device is authorized to communicate with. Public safety agencies in some regions work collaboratively to assign unique ranges of these ID numbers to each agency and system. This approach can minimize confusion when duplicate ID numbers are assigned while also allowing for faster translation of Talker ID data (e.g., Engine 31's mobile radio uses the same Talker ID when transmitting on any radio network in their region).

Talker ID is also the cornerstone of the Emergency Call Button feature which is used by first responders to request immediate assistance.

Public safety agencies currently use a variety of approaches and methods in managing Talker IDs on existing LMR systems:

- Display of Unit ID is controlled by the LMR system administrator who can determine which devices and consoles receive PTT IDs.
- Some agencies transmit the basic Talker ID radio number and require dispatchers to look up the fixed assignment of the device in a spreadsheet or by using an online resource.
- Some agencies program an alias identity into the network that will translate the Talker ID into a more coherent identity (e.g., translate Radio ID 700012345 to "Engine 36" or "Patrol 203").
- Some agencies interface their LMR radio network and their CAD systems and provide dynamic ID translation:
    - An officer signs into their CAD system Mobile Data Client with their CAD system ID ("1Adam12"). They also enter their badge number (#1234) and their vehicle number (V610).
    - Talker ID assignment tables in CAD then create a real-time translation of the various radio devices used by the officer. An incoming radio ID is translated to determine which vehicle it represents. The CAD system then looks to see which

officer is currently assigned to that vehicle. If the officer keys up their mobile radio, the incoming Talker ID for the mobile radio is converted to the officer's CAD Unit ID and "1Adam12" is displayed to the dispatcher. If the officer keys up their portable radio, the incoming Talker ID for the portable radio is converted into the officer's CAD Unit ID and "1Adam12" is displayed.

- Some LMR systems (non P25) allow for alias ID to be transmitted over the air. This includes MDC1200 signaling as well as DMR and NexEdge. Some systems support a static (fixed) alias and other systems dynamically assign an alias based on a subscriber log in.

In the NPSBN environment, instead of independent local, regional, and statewide radio networks, a single nationwide network will be created. This will, for the first time, allow nationwide interoperability between first responders units and devices. The NPSBN will have to support the provision of meaningful LTE Talker IDs for all users, including users who are out of their local area. For example, a city police officer may need to make radio contact with a local Sheriff's Office to get assistance as they are traveling outside their assigned jurisdiction. The LTE Talker ID of the police officer should be sufficiently detailed to allow the public safety agency receiving his transmissions to identify his agency affiliation and/or personal identity.

The ability to interoperate with secondary responder agencies will also require LTE Talker ID coordination. Transportation, public works, and other Extended Public Safety users may be supporting a major incident and need to communicate with law enforcement, fire, and EMS units. The exchange of Talker ID information should allow a user to determine the identity of the agency they are communicating with and the identity of the specific unit within that agency.

The same usage pattern for LMR will occur with LTE devices. First responders may use multiple LTE devices during their duty shift. A police officer may use a vehicle based LTE radio, a portable LTE radio, and an LTE tablet. All of the devices will need to identify the officer as the device "user" and further identify which device the officer is using at that instance. The need to identify the device that is transmitting provides an additional element of safety. If an officer calls for help at an unknown location, it is important to know if the transmission originated from their vehicle (parked in front of the apartment building) or from a device carried on their person.

From an LMR to LTE interoperability perspective, it should be noted that LTE devices will support a more robust Talker ID data structure than P25 devices. This gives LTE devices the ability to transmit more characters of information than is possible on P25 networks today. Talker ID (and Emergency Call Button data) will need to flow between LMR and LTE interworked systems. The full LTE Talker ID data string may need to be translated into a shorter ID that can

be displayed on a P25 subscriber device or console (based on the limitations of the P25 data string).

LTE supports a number of device and service identifiers including IMEI (used by the carrier for provisioning), IMSI (used by the carrier for certain service aspects), and the SIM card. 3GPP standards also support an MCPTT ID and an Alias ID. In this context, "Talker ID" is meant to identify the first responder for public safety purposes (e.g., Officer Jones, Badge Number #9999, who today is assigned the CAD Radio Call Sign "1Adam12" and is riding in patrol car V1234).

LTE Talker ID must also support an alias for a device not associated with a first responder (e.g., Seattle PD Vehicle #1234). LMR radio devices today may be used in an emergency by a first responder who is not on duty and is therefore not logged into the CAD system. Public safety agencies need to be able to identify devices in use which are not associated with a first responder, either to assist them in an emergency or to detect lost and stolen equipment.

Public safety agencies also respond to incidents and coordinate with a variety of other entities, including school security personnel, transit agency supervisors, and others. In certain cases, it may be beneficial to exchange Talker ID information with those other entities. Each agency would need to make their own decision as to whether they would share this data bi-directionally and with whom.

Based on the information contained in this chapter, the following public safety technical requirements were identified.

#	Requirements
11*	A nationwide standardized approach to the assignment of LTE Talker ID and LTE Alias ID SHALL be implemented to ensure that the displayed information has meaningful context for first responder agencies.
12*	LTE devices and consoles SHALL support and display an alias identity that will provide a functional description of the device user with greater detail than is available from the IMEI (LTE device ID) and IMSI (LTE subscriber ID).
13*	Talker ID of the first responder SHALL be fully supported even if the first responder is transmitting through an LTE relay.
14*	The Talker ID data stream SHALL identify which device the first responder is using when they communicate (e.g., transmitting from their vehicle LTE device, their portable LTE device, etc.)
15*	First responders SHALL be able to view the Talker ID Alias that is assigned to their

	device to verify it is correct.
16*	First responder devices and consoles SHALL support a display of recent Talker ID Alias for devices that have transmitted on their talkgroup.
17*	The Talker ID and Talker ID Alias data stream SHALL be designed around open standards in order to interoperate with existing public safety agency systems, including CAD.
18*	A default Talker ID Alias SHALL be supported which will identify devices that are not associated with a specific first responder (e.g., a vehicle device where the first responder has not yet signed on). This Alias should, at a minimum, identify the agency assigned to the device, the device type, and any inventory information (e.g., vehicle number).
19	Based on local control preferences, Talker ID data SHOULD be available when first responders are interconnected with Extended Primary Public Safety users.
20	Based on local control preferences, Talker ID data SHOULD be available when first responders are interconnected with users on other external networks (e.g., school security officers).
21	A standardized nationwide hierarchy governing the assignment of LTE talkgroup IDs SHALL be designed to create a meaningful assignment and to prevent introduction of duplicate IDs.

4.3.4 EMERGENCY

As stated in the prior section, Talker ID is also the cornerstone for the Emergency Call Button feature which allows a first responder to request immediate assistance. In an LMR environment, activation of the Emergency Call Button may be done manually (where an officer presses and holds the red button on the top of the radio) or may be done automatically (where the radio device senses that the officer is down and not moving). There is ongoing research into the development of new technologies in which sensors will automatically trigger the Emergency Call Button. Several manufacturers are already deploying some of these solutions which include motion and imaging sensors that can detect if a first responder is in a fight or struggling with someone, can detect if an officer fires their weapon, or if a vehicle crash is detected.

Public safety agencies can customize the behavior of their LMR Emergency Call Button and will expect the same capability with LTE devices. There are a number of different configurations for

this feature and some agencies use more than one approach within the same radio (based on which radio network the device is connected to). In some instances, activation of the LMR Emergency Call Button will cause the radio to "revert" to a specific emergency talkgroup. Other agencies program their LMR radios to transmit the emergency signal on the talkgroup that is currently selected. Other agencies may have their radio automatically select an emergency talkgroup when the radio is connected to the home agency system, but have the emergency alert transmitted on the selected talkgroup when the device is connected to neighboring radio networks. This flexibility is necessary in order to meet the unique operational needs of each public safety agency.

In an LTE environment, a larger amount of identification data can be transmitted with the emergency alert than is possible with a P25 LMR system. It is important that sufficient data be transmitted to fully identify the first responder in distress. Given the nationwide interoperability of the NPSBN, an itinerant public safety user may need emergency assistance while traveling in an adjoining state. Activation of the Emergency Call Button on their LTE device should trigger an alert to the closest PSAP or a PSAP designated to receive these alerts for the city, county, or region. Activation of the LTE Emergency Call Button should also result in an alert message reaching the first responder's home agency.

Just as Talker ID data should be exchanged between units and PSAPs who are using interworked LMR and LTE talkgroups, Emergency Call Button data should also be exchanged between LMR and LTE interworked talkgroups.

It should be noted that the Emergency Call Button features and capabilities are significantly different in LTE and the information in this chapter should not be construed as representative of all issues that need to be addressed. For example, how should LTE Emergency Call Button alerts be acknowledged and disabled? What additional options may be available for audible and visual alerts based on the uniqueness of the LTE device? How is user device location data leveraged to support the Emergency Call Button event?

Based on the information contained in this chapter, the following public safety technical requirements were identified.

#	Requirements
22*	LTE Emergency Call Button functionality SHALL be configurable by the local public safety agency, including automatic reassignment to a dedicated Emergency Talkgroup or having the first responder remain on the selected talkgroup. Those features should be configurable on a talkgroup by talkgroup basis to allow consistent behavior with neighboring agency policies.

23*	The LTE Emergency Call Button alert SHALL display similar information that is contained in the Talker ID/Alias ID, including the first responder's assigned ID, their agency, and information on which LTE device triggered the emergency alert.
24*	The LTE Emergency Call Button SHALL transmit the data alert to other LTE devices on the same talkgroup, to the console assigned to the LTE Talkgroup, and to the first responder's home agency console (if different). [LTE to LTE]
25	The LTE Emergency Call Button SHALL transmit the data alert to designated LMR subscriber devices operating on the same interworked talkgroup. [LTE to LMR]
26	An LMR Emergency Call Button SHALL transmit a data alert to designated LTE subscriber radios and LTE consoles operating on the same interworked talkgroup. [LMR to LTE]
27	Based on local control preferences, Emergency Call Button alerts SHOULD be shared when first responders are interconnected with Extended Primary public safety users.

4.3.5 ENCRYPTION

Many public safety agencies employ encryption on their Land Mobile Radio systems to prevent unauthorized disclosure of confidential and sensitive information. Law enforcement agencies are increasingly using encryption during high risk incidents to prevent monitoring by criminal elements and the news media. In several recent cases, media organizations (and even private citizens) have released sensitive tactical information as events were unfolding. Fire and EMS agencies frequently need to conduct private communications with hospital emergency departments during patient treatment. It is frequently necessary to transmit the patient's name over the radio to allow a physician to access their electronic medical records, to view current medications, or to review the patient's most recent 12 lead ECG.

There are a variety of encryption methodologies, including those which are standards based and others that are proprietary to a specific vendor. A number of factors influence successful encryption including the use of shared encryption keys and other configuration and provisioning parameters. The U.S. Department of Homeland Security (DHS), Office of Emergency Communications (OEC), has published several reports[20] which provide information and best practices in this area.

[20] https://www.dhs.gov/safecom/blog/2016/10/12/fpic-releases-encryption-documents

Public safety agencies using the NPSBN may need to conduct encrypted communications with other first responders operating on LMR networks. Joint operations involving agencies who are using both LMR and LTE technology will become a daily occurrence as MCPTT is adopted. Public safety agencies may also desire to have interoperable encryption between their LMR system and early Push to Talk POC solutions offered by FirstNet. As with current LMR systems, public safety agencies need to control which users have access to encryption while also managing the assignment of encryption keys. It should be noted that multiple encryption keys and interoperable talkgroups may be needed by a single agency. A police department SWAT team may require a separate encryption key from the one being used by a specialized gang unit conducting surveillance. Separate encryption keys might also be required by the same agency to restrict access to voice communications between paramedics and hospitals.

Comprehensive training for all first responders, including telecommunicators, on the technical, operational, and policy aspects of encryption is essential. Access to an encrypted communications channel should be seamless for the first responder and should not require manual adjustment of controls on the user's LTE device. If a first responder using an LMR device needs to join an encrypted LTE talkgroup, the technical set up (or transition) of the talkgroup should be managed automatically. It is also important that first responders be alerted to any failure of the interoperable encryption solution. This would allow public safety personnel to modify their message exchanges or move to a different encryption solution.

The technical complexity surrounding the implementation of encryption becomes more significant when you interconnect LMR and LTE networks. The following information provides a high-level overview of the differences between LMR and LTE encryption.

Types of LMR Encryption: In general, digital voice encryption is either based on standards or is provided by a manufacturer as a proprietary feature. Successful interoperability requires the use of a common encryption type as well as successful provisioning of the subscriber devices.

The currently accepted standard for encryption is the 256-bit "Advanced Encryption Standard," also known as AES-256. AES is the designated encryption standard for U.S. federal government agencies and is recommended for use by all public safety agencies. A number of vendor proprietary encryption systems are also in use across the United States. These offer varying degrees of message security and interoperability.

Types of LTE Encryption: LTE encryption functions differently than LMR encryption and can be implemented in several ways depending on the level of message security that is required. There are many technical aspects to LTE encryption at the device, application, and network level. This report will focus on two general approaches to LTE encryption:

- Over the Air Interface encryption only provides secure communications for those portions of the message that are broadcast between the user device and the radio tower.[21] Messages may then traverse the fixed portion of the network without encryption.
- End-to-End encryption occurs at the application layer and maintains the security of the message as it moves from the application on the user's device to other destinations. This is also called "application level encryption.[22]"

Encryption between LMR and LTE Systems: There are two technical approaches to managing encryption of voice communications when LMR and LTE systems are interconnected:

- LMR/LTE Common Encryption: This requires the use of the same encryption and voice coding components on both the LMR and LTE devices, including the encryption algorithm, encryption key, and vocoder. This prevents the need for transcoding between different encryption and vocoder systems.
- LMR/LTE Dissimilar Encryption: This involves the use of one type of digital encryption and vocoder on the LMR network and a different type of encryption and vocoder on the LTE network. When LMR and LTE networks are joined, a decode/recode of the message is necessary at the point of the interconnection. This could produce a security vulnerability if the interconnection point is not properly secured and may cause some voice quality degradation. This approach may also add latency to the communications exchange.

LMR/LTE Interconnection and Encryption Issues: Before LMR-LTE encryption can occur, the two networks must be connected. There are several ways to connect LMR and LTE networks and each solution may offer different levels of operational capability. Certain solutions may not support robust encryption. Interconnection of LMR and LTE systems may occur at the core network (e.g., the infrastructure level) or may occur in the field using specialized devices (e.g., an IP gateway on a mobile command vehicle).

3GPP is currently defining standards to support LMR and LTE interworking. Their focus is on the LTE side of the interworking solution and they are defining a data interface that will share specific components of the MCPTT system. Other organizations, including ATIS and TIA are working to develop standards for the LMR side of the interworking solution that will interoperate with the 3GPP interface. The use of non-proprietary, open source standards is important to enable a range of solutions to meet different agency needs.

Existing technologies that interconnect disparate LMR systems may be used to achieve interworking between LMR and LTE networks, which may help facilitate encryption. An LMR-LTE interworking solution involving a P25 radio network may leverage a number of existing

[21] Known as the eNodeB.
[22] This involves encryption from the user device/client application to the application server.

interface solutions, including the Inter RF Sub-System Interface (ISSI), the Console Sub-System Interface (CSSI), and the Digital Fixed Station Interface (DFSI).

It should be noted that while many agencies use the P25 standard in their LMR radio systems, other public safety agencies use proprietary trunked solutions or operate using legacy conventional radio systems. LMR-LTE interworking for non-P25 networks may require a separate solution to effectively interoperate with LTE. Console patching and other audio gateway solutions may be leveraged to interconnect analog and proprietary digital communications networks with LTE systems. This should occur using open standard LMR interfaces including P25 CSSI.

End-to-end encryption was viewed as the preferred method in joint LMR LTE operations for a number of operational and technical reasons. This requires the utilization of a common vocoder[23] and common encryption scheme. Two potential solutions[24] were reviewed by the Working Group that would allow end to end encryption.

- First responders would be directed to an interoperability talkgroup designated for encryption. The LTE system would be preconfigured so that LTE users are automatically steered to use a P25 vocoder and P25 encryption scheme.
- If a dedicated LMR/LTE encryption talkgroup is not used, then a solution is needed to manage the addition of a P25 LMR user who is being added to an encrypted LTE talkgroup. During call set up, following the arrival of an LMR P25 user, the LTE network would do a negotiation and change the vocoder of the LTE first responders to match the P25 vocoder and encryption scheme.

Other methods of joint LMR-LTE encryption may result in the need to transcode the message as it crosses the network interface. A first responder may be using one type of encryption on their LMR system and need to communicate with another first responder who is using an LTE encryption methodology. Each transmission is decoded from one encryption scheme into a clear message and then re-coded with the encryption scheme of the other network and passed to that user. This is an acceptable technical solution if network security considerations are managed and the implementation meets the operational requirements of the public safety agencies including issues of latency and voice audio degradation. Any interconnection of LMR and LTE systems requires careful engineering analysis to reduce latency and maximize the performance of message transfer.

These approaches would require several technical components in the interworking solution:

[23] It should be noted that P25 networks use a different vocoder than LTE networks. 3GPP has also identified AMR Wideband as the common vocoder to be used for LTE mission critical voice.

[24] There are a number of different component and configuration options to achieve this result.

- The interworking solution needs to support transcoding, in order to manage the use of disparate encryption solutions (where the LMR system and the LTE system are using different encryption solutions).
- The interworking solution needs to be able to provision new encryption keys.
- The interworking solution needs to support the late entry of users:
    - Late entry of a P25 LMR user into an LTE encrypted talkgroup.
    - Late entry of an LTE user into a P25 LMR encrypted talkgroup.

Beyond those technical elements, the following issues need to be assessed during the discussion on encryption management.

The current 3GPP standard does not support local control of encryption keys. However, work is underway in Technical Standard 23.283 to provide local management of encryption. This would presumably allow all aspects of encryption, including key management, to be handled by the local public safety agency. Requiring encryption management to be handled by the NPSBN operator would likely be viewed as unacceptable to public safety agencies which need to ensure secure communications among authorized users and who manage their LMR encryption keys today. A process will be needed for encryption key management involving regional and statewide encrypted talkgroups which are shared among multiple entities. DHS OEC has identified a recommended strategy to manage these issues within LMR networks. That same approach may be applicable to LTE encryption.

It is recommended that encryption be implemented at the application level to provide end-to-end continuity of message security. The use of "over the air" encryption solutions may not provide the necessary level of message security.

If a first responder's LTE device supports encryption and is stolen, it may be necessary to rekey the encryption algorithm of all other users to maintain secure communications.[25] Encryption keys must also be changed on a regular basis to maintain security of communications. 3GPP has defined encryption key management practices for LTE networks and TIA has defined encryption key management practices for P25 LMR systems. Additional work is needed to determine how these two standards will interoperate. It is preferred that encryption key updates occur over the air rather than require that the device be physically accessed to perform the update.

Encryption between groups of first responders who are operating on both the NPSBN and on a Push to Talk over Cellular (POC) network has not been addressed, nor has encryption between first responders operating on NPSBN, POC, and LMR simultaneously.[26] Local public safety

[25] While it may be possible to remotely disable the stolen device, some high risk tactical operations would require distribution of a new encryption key.
[26] These issues are being noted in the report, but are considered out of scope for this document.

agencies may determine that they need encryption capabilities with users on these alternate networks.

The use of P25 "multi-key" supports the transition period between the time a new encryption key is released until all LMR subscriber devices are updated. Tactical voice communications may need to continue during the subscriber device update process. 3GPP standards need to address how this will occur during an LMR/LTE interconnection (where two valid LMR encryption keys are in use simultaneously).[27]

LMR Link Layer encryption relates to voice and data payload encryption including ID translation across the interworking interface. In a P25 system, the Device ID and Talkgroup ID may be encrypted.[28] Public safety agencies may desire to have these same data elements secured on the LTE network.

While this report deals with Mission Critical Voice issues, it is important to note that encryption of all data, including message traffic, video, and application data is necessary for certain public safety operations.

Further examination of these issues by public safety is warranted and a recommendation on this topic is included in Chapter 5.

Based on the information contained in this chapter, the following public safety technical requirements were identified.

#	Requirements
28	First responders and consoles using LMR and LTE interconnected talkgroups SHALL be able to conduct encrypted voice communications.
29	Designated LMR and LTE interconnected talkgroups SHALL be able to support secure voice and data communication using an "end-to-end" encryption solution.
30	Designated LMR and LTE interconnected talkgroups SHALL be able to support secure voice and data communications using either a common encryption solution or a transcoded encryption solution based on local agency needs.
31	First responders SHALL not be required to take any special action to encrypt their communications when accessing a designated encryption talkgroup which includes users from an alternate network (e.g., LMR and LTE).

[27] 3GPP standards do not address multi-key for LTE.

[28] On LMR, encrypted communications include the device ID and the Talkgroup ID. In a transcoded environment, these data elements have to be exposed at the interworking interface in order to be passed on to the other network. P25 is currently working on this issue.

32	First responders and consoles SHALL be alerted if an encrypted talkgroup loses its encryption capability.
33*	Local control policies SHALL determine which users and user devices are authorized to access and engage in encrypted communications.
34*	A number of different encryption keys SHALL be available to public safety agencies in order to segregate different groups of users within a single agency.
35*	Encryption key management for systems and applications used by public safety agencies SHALL be handled by an authorized representative of the local public safety agency or their designee.
36*	Encryption key management for regional, statewide, and nationwide encrypted LTE talkgroups SHALL be managed by a designated coordinating entity.
37	Public safety agencies SHOULD be able to distribute new or replacement encryption key data (encryption re-keying) with LMR and LTE user interconnected devices without having to physically access the device.

4.3.6 SCAN

Today, most public safety agencies implement a scanning capability on their LMR networks to allow first responders to monitor radio activity on more than one channel or talkgroup. The ability to maintain situational awareness of day-to-day operations or a major incident is enhanced with this functionality. In LMR, a sequential scan process is used where the subscriber radio monitors for activity on a set of channels and stops to provide audio if a channel is active. When radio traffic on that channel is complete, the radio continues scanning. While the sequential scan method is not perfect and can miss transmissions, the benefits of its use outweigh the limitations of the technology.

This same scan capability will be needed on LTE devices supporting Mission Critical Voice. The 3GPP standards for Mission Critical Voice provide for the simultaneous delivery of multiple audio streams from selected LTE talkgroups. This capability would allow a first responder to hear radio traffic on the dispatch talkgroup while also hearing radio traffic from the fire ground talkgroup. The provision of simultaneous audio solves one problem (e.g., no missed transmissions) but creates a new problem (e.g., how to manage multiple audio streams so they can be intelligible). This capability may be implemented in different ways by industry, including an option to raise the audio level of a priority talkgroup above the audio level of the monitored talkgroups; muting the audio stream of the monitored talkgroups when a transmission is received on the priority talkgroup; or allowing for some type of spatial separation of radio

traffic through the use of multiple speakers. It is also possible that manufacturers will implement the LMR "serial scan" solution on the LTE devices in order to mirror the current day-to-day operation.

It should be expected that first responders will be jointly operating on incident scenes using both LMR and LTE technology. The Incident Commander will need to scan radio traffic from interworked talkgroups supporting both technologies. Today, some Incident Commanders use two (or more) radio devices with each one tuned to a specific talkgroup. Other Incident Commanders rely on the scan functionality and still others use a combination of both approaches.

Features and functionality present with LMR scanning will be needed in the LTE scan solution. This includes the ability to assign a set of talkgroups to a fixed scan list or allow the first responder to create an ad hoc scan list in their radio. An Incident Commander may need to react to a radio transmission that is heard while scanning multiple talkgroups. They may need to transmit a message on the scanned talkgroup (which could be different than the talkgroup selected on their device). The LTE scan solution needs to support the ability for an Incident Commander to quickly transmit on a scanned talkgroup.

Based on the information contained in this chapter, the following public safety technical requirements were identified.

#	Requirements
38	First responders SHALL have the ability to monitor multiple LTE talkgroups to maintain situational awareness of the incident, including interworked LMR/LTE talkgroups.
39	First responders SHALL be able to scan both static interworked talkgroups (which are configured in advance) and dynamic talkgroups (which are created on an as-needed basis).
40	First responders SHALL have the capability to designate a priority talkgroup, which will distinguish the priority talkgroup audio over the radio communications of other talkgroups being received.
41	Local control policies SHALL allow the public safety agency to configure the scan features at the time the device is provisioned for use.
42	LTE scan capabilities SHALL meet or exceed the features available on existing LMR

	P25 networks.
43	While scanning, first responders SHALL have the ability to easily transmit on a talkgroup other than the selected/priority talkgroup.
44	First responders using LMR subscriber devices on an LMR/LTE interworked talkgroup SHALL be able to receive sequential scan audio from other interworked LTE talkgroups.

4.3.7 FULL DUPLEX

By design, all Push to Talk networks are half duplex in which the radio is either listening for audio or is transmitting audio. Full duplex voice communications occur when both incoming (from the caller) and outbound audio (from the user of the device) are supported simultaneously. The easiest example of full duplex involves telephone calls, in which both parties can speak at the same time.

Full duplex voice also allows for "hands free" operation, since there is no need to "push to talk." This technology would allow a paramedic to conduct a two-way conference call with an Emergency Department physician while using both hands to start an intravenous line on a patient. Full duplex voice may also be used with video calls, including those initiated from a first responder's body camera.

In LMR, full duplex plays a critical safety role by allowing the telecommunicator to "listen" to radio traffic from field users at the same time they are transmitting a message. This provides a "dispatcher override" feature which can be essential in communicating urgent orders to evacuate a structure or to provide information to field units when a radio microphone is stuck open. This capability must be sustained during the interconnection of LMR and LTE talkgroups for joint operations.

LTE technology will provide for full duplex voice communications between LTE users. There may also be certain unique situations where public safety agencies would need full duplex communications between interworked LMR and LTE users. It is recognized that there are technical limitations restricting how this may occur.

Based on the information contained in this chapter, the following public safety technical requirements were identified.

#	Requirements
45	LTE consoles SHALL support full duplex voice to permit a telecommunicator to override first responder voice traffic on LTE talkgroups and LMR-LTE interworked talkgroups.
46*	First responder LTE devices SHALL support full duplex voice conversation with other users on the LTE network.

4.3.8 LTE CONSOLES

Today, public safety LMR radio consoles provide a wide range of essential functionality to manage voice communications. While some LMR consoles are connected using wireless technology,[29] most consoles are hard wired into their network infrastructure. Almost all new consoles are designed using IP based technology. Today, LTE technology does not have an equivalent wire line console and 3GPP standards have not defined a public safety console.

The word "console" refers to any public safety command and control system. While these are primarily located in dispatch centers and Public Safety Answering Points (PSAPs), specialty consoles may be located in other facilities, including agency Emergency Operation Centers (EOCs), hospital Emergency Departments, and Trauma Centers. It is further recognized that some of these specialty LTE consoles will be used at the scene of major incidents and may exist as either wired or wireless console devices.

For example, an Incident Commander may have a specialty console in their vehicle which might be a larger wireless device that will have unique requirements. These may include the need to support multiple independent speakers to spatially manage incoming audio from multiple talkgroups. Specialty devices and consoles should support audio record and play back functionality to help manage multiple audio streams.

Specialty devices and consoles will have unique requirements that were not addressed in the development of requirements for this report. NPSTC published a report on *Public Safety Broadband Consoles* in September of 2014 which identified 54 requirements.

Voice and data logging system interfaces are needed to capture and store audio and metadata for retention purposes and this capability should be designed to maintain parity with existing LMR consoles. NPSTC should consider tasking the LMR LTE Interoperability and Integration Working Group to examine needed capabilities and features on consoles to support LMR-LTE interoperability as well as a review of general LTE console needs.

[29] This typically involves connecting the remote console device to a subscriber or donor radio.

5. Conclusions and Recommendations

This chapter is designed to provide high-level conclusions and a set of basic recommendations regarding the provision of mission critical voice services by the NPSBN operator and the use of these services by public safety personnel. Following the review of multiple use cases and after discussion with public safety agency representatives, a number of conclusions and recommendations have been identified:

1. **Mission Critical Voice services are an essential element of the NPSBN.** They include group communications services, including MCPTT, full duplex voice communications, and full duplex video chat. FirstNet, through its partnership with AT&T is accelerating the activation of the NPSBN and introducing non-mission critical PTT service[30].
    - ***Recommendation**:* The SAFECOM Interoperability Continuum should be used for guidance during all phases of implementation, and on an ongoing basis. Beyond the Technology lane of the Continuum, attention must be paid to Training, Governance, SOPs, and Usage. Attention to the Continuum lanes will be important to the successful implementation of these technologies.
    - ***Recommendation*:** FirstNet should help inform users that interim POC solutions should not be considered a replacement for critical voice communications provided by LMR, and that reliance on POC PTT solutions for primary voice communications should wait until 3GPP-compliant MCPTT is deployed and found to meet public safety objectives.

2. **Public safety agencies expect the NPSBN to support a robust multi-vendor ecosystem, and the availability of a wide range of user devices, equipment, and services using non-proprietary, open standards**. FirstNet must ensure that implementation of the NPSBN does not inadvertently create an unfair monopoly caused by equipment[31] and services offered only by a limited number of manufacturers.
    - ***Recommendation***: FirstNet should fully document their requirement for interoperability between and among devices and applications, including the use of APIs to help ensure a multi-vendor ecosystem.
    - ***Recommendation**:* Until appropriate standards exist for LMR-to-LTE integration, FirstNet should carefully evaluate PTT solution offerings to maximize the availability of multi-vendor solutions and prevent proliferation of proprietary LMR interfaces.

[30] The timeline for MCPTT availability is dependent on a number of factors, including finalization of 3GPP standards, availability of subscriber devices, and network engineering.
[31] See Item #7 below regarding the applicability of console systems to this recommendation.

3. **Integration of LMR and LTE network PTT services is required to support interoperability between users of both networks.** First responders will continue to need to communicate with other public safety agencies who may be using disparate networks,[32] and with personnel from their own agency who are using both platforms. Interoperability solutions should carry data as well as voice traffic to allow sharing of PTT ID, Emergency, and other features.[33] There are many ways to bridge these networks together and use of open standard-based solutions will be essential to prevent implementation of proprietary systems that may not support interoperability with other agency systems. Standardization of this integration effort is critical to ensure that interoperable solutions are implemented nationwide
    - ***Recommendation:*** ATIS/TIA should restart work in Subcommittee TR 8.8 on LMR interworking standards as soon as possible in order to define the standardized features and capabilities for LMR system interconnection with MCPTT.
    - ***Recommendation:*** FirstNet should advocate for accelerated work within 3GPP to address these interconnection issues between LMR and LTE networks
    - **Recommendation**: FirstNet should advocate for the inclusion of multiple open standard methods of LMR-LTE integration[34] while work continues on a 3GPP/TIA fully standardized solution.
    - ***Recommendation:*** FirstNet should require that all non-standards based products and devices be upgraded within a specified period of time following adoption of the relevant standard.

4. **3GPP Standards on direct mode communications are not keeping pace with the speed of deployment of PTT networks**. In addition to accessing an LMR-LTE interoperability solution, first responders must have a robust local area off-network MCPTT communications capability that will allow uninterrupted service during a failure of network infrastructure, or when a responder transitions into an area without NPSBN coverage. In the absence of a standardized solution, vendors are introducing their own products that provide direct mode voice. These solutions may not be interoperable with each other and may result in non-standards based solutions being introduced into the NPSBN. Public safety agencies should understand that some solutions may provide interim direct mode communications while standards work is completed.
    - ***Recommendation:*** FirstNet should articulate a roadmap for direct mode voice communications and how early vendor-offered solutions will integrate with a future nationwide direct mode standard.

[32] First Responders may also be using WIFI, 4.9 GHz, and other bands.
[33] Current work in 3GPP will define which features and capabilities are exposed at the LMR/LTE interface.
[34] These include the P25 Inter RF SubSystem Interface (ISSI), the Console SubSystem Interface (CSSI), the Bridging Systems Interface (BSI), the P25 Conventional Digital Fixed Station Interface (DFSI) and use of donor radios.

5. **Digital voice encryption is an important component for certain MCPTT communications on interworked LMR-LTE networks and must be considered when planning LMR-LTE integrated channels**. There are many technical and policy issues surrounding encryption of LTE voice communications and encryption becomes more complicated when joint LMR-LTE talkgroups are involved and there is a need for "end-to-end" encryption.
    - ***Recommendation***: FirstNet should publish guidance on how encryption will be managed on the NPSBN, including encryption of PTT and MCPTT communications and the supported options for managing encryption when LMR and LTE networks are interconnected. This guidance should include instruction on the need for LTE devices to support the P25 vocoder[35] to enable end-to-end encryption.

6. **Video chat function with full duplex voice is an important capability for first responders**. For example, EMS personnel may need to do a hands-free consultation with a medical control physician. Law enforcement and fire personnel will also make use of this function in a variety of settings. 3GPP work on Mission Critical Video should be monitored for future implementation to supplement MCPTT services.
    - ***Recommendation***: FirstNet should also require vendors to differentiate between a standard video chat offering and a Mission Critical Video chat offering.

7. **LTE consoles play an important role in the evolution of PTT service and MCPTT services**. PSAPs may begin using POC applications to support administrative functions. This will require tight integration with existing LMR console equipment. The implementation of MCPTT will further require a purpose-built console device supporting a rich set of features and capabilities. Integration of LMR and LTE communications is essential, and some aspects of this function may be managed at the console level. Connection and interworking components to support LTE console functionality are not yet defined in 3GPP standards. As the Act requires the integration of PSAPs,[36] PSAP systems, such as dispatch consoles, must also be among the equipment for which open standards recommendations apply.
    - ***Recommendation***: Additional first responder input is needed to help define needed capabilities for these devices. NPSTC produced an early report on LTE console functionality[37] that should be refreshed.
    - ***Recommendation***: FirstNet should advocate that 3GPP define a wireline dispatch interface for MCPTT if the evolving 3GPP interworking standard for LMR

[35] Availability of the P25 vocoder in LTE subscriber devices is required to support certain interworking solutions, beyond the need for encryption.

[36] Section 6202(b)(2)(B)(ii)

[37] See NPSTC LTE Console Report

and LTE does not meet public safety's expectations. This same approach may be needed to obtain wireline interfaces to manage Mission Critical Data and Mission Critical Video.

During the development of this report, several key issues were identified that were outside the Working Group's focus on LMR-LTE interoperability. However, those issues are both important and indirectly impact LMR-LTE integration. They are noted below with a recommendation for follow-up action.

1. **Digital voice encryption is an important component for certain communications occurring exclusively on MCPTT talkgroups.** Certain technical, standards, and policy issues must be addressed and more information is needed on how encryption is managed on a nationwide network and to what extent local public safety agencies will have control over management of local encryption keys. Most public safety agencies tightly manage these resources and limit the sharing of encryption keys with other agencies. However, the NPSBN will allow nationwide MCPTT interoperability and thus introduce challenges with the effective implementation of encryption.
    - ***Recommendation*:** NPSTC should task the LMR LTE Integration and Interoperability Working Group to further study this issue.

2. **Work is needed to assess technical and policy issues regarding the creation and management of LTE talkgroups**. As the Working Group was discussing the need to interconnect LMR and LTE talkgroups, it became apparent that the NPSBN will be supporting thousands of LTE talkgroups. Management of LTE talkgroups, including Talkgroup IDs and Talkgroup Aliases are needed to prevent technical and operational challenges involving duplicate IDs and names.
    - ***Recommendation*:** NPSTC should task the LMR LTE Integration and Interoperability Working Group to further study this issue.

3. **A nationwide standard is needed to define creation of PTT IDs by public safety agencies**. As the Working Group was discussing the need for MCPTT IDs to be exchanged with LMR PTT IDs, it became apparent that a standard will be needed to manage this information. This includes procedures for regionalization of nationwide LTE talkgroup coverage and the establishment of regional (state or multi-county) LTE interoperability talkgroup standards. FirstNet is providing a nationwide interoperable communications network that will allow first responder devices to operate virtually anywhere. The identity of the first responder is a critical safety feature and some form of identification is needed for itinerant users who have traveled outside of their home agency service area.
    - ***Recommendation***: NPSTC should task the LMR LTE Integration and Interoperability Working Group to further study this issue.

- ***Recommendation***: FirstNet should identify technical solutions for the provision of PTT ID, including whether Over the Air Alias (OTAA) is an appropriate solution.

1. **A standard is needed for nationwide LTE Interoperability talkgroup names**. LMR networks today support access to a set of FCC-designated nationwide interoperability channels. These allow a first responder to communicate with local agencies while they are out of their home agency service area. Nationwide LMR interoperability channels have ANSI standardized names to ensure that first responders from different agencies can locate the desired channel in their radio. A similar set of nationwide interoperable LTE talkgroups will be needed to mirror the existing LMR function. Those LTE talkgroups must have standardized channel names to create a common identity in all user devices.
    - ***Recommendation****:* NPSTC's Common Channel Naming Working Group, which authored the ANSI standard for designated channel names for nationwide LMR channels, should continue their work to identify suitable names for nationwide interoperable LTE talkgroups and investigate viable options for implementation of regional coverage solutions.

2. **MCPTT interoperability requirements must be considered**. As the Working Group was discussing LMR-LTE interoperability it became apparent that first responders will require the same level of interoperability when operating on different LTE networks. Public safety agencies require interoperability with other public safety agencies and responder organizations regardless of their network, technology, or spectrum band. Interoperability is as important between LMR and LTE as it is between different LTE networks. NPSTC recently completed a comprehensive report on the use of Broadband Deployable Systems which was done as a cooperative effort with the Canadian government. A key take away from that report was the need for seamless interoperability between first responders on both sides of the international border. Public safety personnel need to access and share voice and data communications with other first responders operating at a common incident scene. That report concluded that an LTE core-to-core connection would likely be required between FirstNet and the Canadian Public Safety Broadband Network. This need for interoperability between first responders becomes more complex as additional commercial carriers begin to offer public safety broadband services on their networks.
    - ***Recommendation:*** FirstNet should participate with the European Telecommunications Standards Institute (ETSI) program as they work to define a Compliance Assessment Program (CAP) to ensure interoperability between different devices and services provided by different manufacturers.

3. **Public safety agencies need to better understand how the NPSBN will be operated and decisions on the adoption of 3GPP standards.** There is uncertainty in how new releases of 3GPP standards will be implemented by manufacturers and network operators. For example, a 3GPP standard that describes the MCPTT Scan/Monitor function provides for simultaneous receipt of multiple audio streams to a user device. Some industry

representatives have stated that LTE scan will be provided as a sequential monitor function – similar to how LMR scan works today. Another 3GPP standard allows first responder user devices, including field supervisors and Incident Commanders, to monitor direct mode communications simultaneously with network based communications. Industry representatives have indicated that the requirement for a dual receiver will significantly change UE device hardware requirements and may not be commercially viable. Both FirstNet, and the public safety agencies it serves, need to understand the expected technical environment that will be supporting their operations.

- ***Recommendation***: FirstNet should inform the PSAC on which public safety requirements noted in 3GPP standards will likely not be supported by the manufacturing community (e.g., chipset, device, and network operators).

4. **Public safety agencies should use caution when evaluating vendor equipment that is designated "mission critical."** Many vendors are using this phrase to market devices and solutions. This may make public safety agencies believe that the device or service is suitable for use by first responders in life and death situations.
    - ***Recommendation****:* FirstNet should articulate how any given NPSBN product or service offering receives a "Public Safety Mission Critical" label, allowing first responders to know that a device/application/service has been independently evaluated and is suitable to perform in an emergency.

APPENDIX A1:
Public Safety Technical Requirements

Chapter 4 - Examination of Public Safety Requirements	
Note - The Working Group also identified requirements that indirectly deal with LMR-LTE Interoperability. These are flagged with an asterisk (*) and have explanatory information included in Chapter 5.	
4.3.1 - Interoperability	
1	First responders operating on LMR and LTE networks SHALL be able to communicate with each other including while responding to the scene of the incident as well as upon arrival.
2	Consoles operating on LMR and LTE networks SHALL be able to monitor and participate in the voice communications on interworked LMR and LTE talkgroups.
3	First responders and consoles SHALL have access to multiple LTE talkgroups to coordinate on scene operations and many of these LTE talkgroups will need to be interconnected with LMR talkgroups to support incident operations.
4.3.2 - Direct Mode	
4*	Local configuration settings SHALL determine the user device's response when it identifies a loss of macro network coverage. The device may be programmed to automatically switch to an agency specified direct mode talkgroup or require that the device be manually switched to Direct Mode.
5*	Local configuration settings SHALL determine which direct mode LTE talkgroup the user's device switches to when it senses a loss of macro network coverage (e.g., does the device switch to a common interoperable LTE talkgroup or a discipline or agency specific LTE talkgroup).
6*	A first responder SHALL be able to manually set their LTE device to remain in a specific mode of operation regardless of the presence or absence of macro network coverage. This includes setting the device to remain on the macro network or setting the device to remain in direct mode.
7*	A first responder SHALL be able to communicate with personnel who are on either the macro network or operating in direct mode. Note - It is recognized that communications in direct mode are range limited. 3GPP provides for a device with a dual receiver, where an Incident Commander at a scene could communicate with the dispatcher using LTE network and also with a nearby first responder who is on direct mode operating inside the building.

8*	First responders (e.g., Primary Public Safety users) SHALL be able to communicate with Extended Primary Public Safety users using Direct Mode (e.g., mass transit supervisor, DOT snow plow, utility worker).
9*	A direct mode emergency broadcast message SHALL reach all devices on all LTE direct mode talkgroups within RF range, including Primary and Extended Primary public safety users.
10*	An emergency broadcast message SHALL reach all FirstNet devices in the immediate area on all macro LTE talkgroups providing an alert to both Primary and Extended Public Safety users.
4.3.3 - Talker ID	
11*	A nationwide standardized approach to the assignment of LTE Talker ID and LTE Alias ID SHALL be implemented to ensure that the displayed information has meaningful context for first responder agencies.
12*	LTE devices and consoles SHALL support and display an alias identity that will provide a functional description of the device user with greater detail than is available from the IMEI (LTE device ID) and IMSI (LTE subscriber ID).
13*	Talker ID of the first responder SHALL be fully supported even if the first responder is transmitting through an LTE relay.
14*	The Talker ID data stream SHALL identify which device the first responder is using when they communicate (e.g., transmitting from their vehicle LTE device, their portable LTE device, etc.)
15*	First responders SHALL be able to view the Talker ID Alias that is assigned to their device to verify it is correct.
16*	First responder devices and consoles SHALL support a display of recent Talker ID alias for devices that have transmitted on their talkgroup.
17*	The Talker ID and Talker ID Alias data stream SHALL be designed around open standards in order to interoperate with existing public safety agency systems, including CAD.
18*	A default Talker ID Alias SHALL be supported which will identify devices that are not associated with a specific first responder (e.g., a vehicle device where the first responder has not yet signed on). This Alias should, at a minimum, identify the agency assigned to the device, the device type, and any inventory information (e.g., vehicle number).
19	Based on local control preferences, Talker ID data SHOULD be available when first responders are interconnected with Extended Primary Public Safety users.
20	Based on local control preferences, Talker ID data SHOULD be available when first responders are interconnected with users on other external networks (e.g., school security officers).
21	A standardized nationwide hierarchy governing the assignment of LTE talkgroup IDs SHALL be implanted as to create a meaningful assignment and to prevent introduction of duplicate IDs.
4.3.4 - Emergency	

22*	LTE Emergency Call Button functionality SHALL be configurable by the local public safety agency, including automatic reassignment to a dedicated Emergency Talkgroup or having the first responder remain on the selected talkgroup. Those features should be configurable on a talkgroup by talkgroup basis to allow consistent behavior with neighboring agency policies.
23*	The LTE Emergency Call Button alert SHALL display similar information that is contained in the Talker ID/Alias ID, including the first responder's assigned ID, their agency, and information on which LTE device triggered the emergency alert.
24*	The LTE Emergency Call Button SHALL transmit the data alert to other LTE devices on the same talkgroup, to the console assigned to the LTE Talkgroup, and to the first responder's home agency console (if different). [LTE to LTE]
25	The LTE Emergency Call Button SHALL transmit the data alert to designated LMR subscriber devices operating on the same interworked talkgroup. [LTE to LMR]
26	An LMR Emergency Call Button SHALL transmit a data alert to designated LTE subscriber radios and LTE consoles operating on the same interworked talkgroup. [LMR to LTE]
27	Based on local control preferences, Emergency Call Button alerts SHOULD be shared when first responders are interconnected with Extended Primary public safety users.
4.3.5 - Encryption	
28	First responders and consoles using LMR and LTE interconnected talkgroups SHALL be able to conduct encrypted voice communications.
29	Designated LMR and LTE interconnected talkgroups SHALL be able to support secure voice and data communication using an “end-to-end” encryption solution.
30	Designated LMR and LTE interconnected talkgroups SHALL be able to support secure voice and data communications using either a common encryption solution or a transcoded encryption solution based on local agency needs.
31	First responders SHALL not be required to take any special action to encrypt their communications when accessing a designated encryption talkgroup which includes users from an alternate network (e.g., LMR and LTE)
32	First responders and consoles SHALL be alerted if an encrypted talkgroup loses its encryption capability.
33*	Local control policies SHALL determine which users and user devices are authorized to access and engage in encrypted communications.
34*	A number of different encryption keys SHALL be available to public safety agencies in order to segregate different groups of users.
35*	Encryption key management for systems and applications used by public safety agencies SHALL be handled by an authorized representative of the local public safety agency or their designee.

36*	Encryption key management for regional, statewide, and nationwide encrypted LTE talkgroups SHALL be managed by a designated coordinating entity.
37	Public safety agencies SHOULD be able to distribute new or replacement encryption key data (encryption re-keying) with LMR and LTE user interconnected devices without having to physically access the device.
4.3.6 - Scan	
38	First responders SHALL have the ability to monitor multiple LTE talkgroups to maintain situational awareness of the incident, including interworked LMR/LTE talkgroups.
39	First responders SHALL be able to scan both static interworked talkgroups (which are configured in advance) and dynamic talkgroups (which are created on an as-needed basis).
40	First responders SHALL have the capability to designate a priority talkgroup, which will distinguish the priority talkgroup audio over the radio communications of other talkgroups being received.
41	Local control policies SHALL allow the public safety agency to configure the scan features at the time the device is provisioned for use.
42	LTE scan capabilities SHALL meet or exceed the features available on existing LMR P25 networks.
43	While scanning, first responders SHALL have the ability to easily transmit on a talkgroup other than the selected/priority talkgroup.
44	First responders using LMR subscriber devices on an LMR/LTE interworked talkgroup SHALL be able to receive sequential scan audio from other interworked LTE talkgroups.
4.3.7 - Full Duplex	
45	LTE consoles SHALL support full duplex voice to permit a telecommunicator to override first responder voice traffic on LTE talkgroups and LMR-LTE interworked talkgroups.
46*	First responder LTE devices SHALL support full duplex voice conversation with other users on the LTE network.

APPENDIX A2:
NPSTC PTT over LTE Report – 2013
Public Safety Technical Requirements

NPSTC Report: PTT over LTE Requirements, 2013	
Requirement Table Extract	
REQ #	**Requirement Statement**
Table 1	Table 1. PTT Group Call Requirements
1	The PTT Service SHALL provide a mechanism by which a UE can make a 1-to- many PTT transmission to any PTT Group for which it is authorized.
2	The PTT Service SHALL provide a mechanism by which PTT UEs can determine the currently active PTT Groups for which it is authorized.
3	The PTT Service SHALL provide a mechanism by which PTT UEs can determine what PTT Groups are being monitored by some other UE, as authorized.
4	The PTT Service SHALL provide a mechanism by which a Public Safety Entity Administrator, from any location, may define the membership of a PTT Group.
5	Public Safety Entity Administrators SHALL have the capability to create a hierarchy for what users, user types, and/or devices can override an active PTT Group transmission.
6	When an authorized user overrides a PTT Group transmission, authorized users SHALL be able to listen to both the overriding and overridden PTT Group transmissions.
7	When an authorized user overrides a PTT Group transmission, a Public Safety Entity Administrator SHALL be able to configure which PTT Group transmission a user receives, overriding and/or overridden.
8	When an authorized user overrides a PTT Group transmission, the PTT Service SHALL provide a means of notifying the overridden talker that the transmission has been overridden.
9	The PTT Service SHALL allow the Public Safety Entity Administrator to designate specific PTT Groups to be inaccessible to other users, including dispatchers or supervisors.
10	PTT Groups SHALL support up to the number (N) of PTT Group members selected by the Public Safety Entity Administrator.
11	The PTT Service SHALL allow a UE to actively participate in 1 PTT Group transmission while simultaneously monitoring additional PTT Group transmissions. [38]

[38] This ability is important to an environment where an emergency message needs to be distributed to those in the field who are monitoring other resources such as an emergency message to immediately evacuate a building. Monitoring multiple talk paths may be beneficial in the distribution of important, real-time information, as needed.

12	The PTT Service SHALL present users with alias or alphanumeric group identifiers [39] for PTT Groups. [40]
13	The PTT Service SHALL provide a notification, for example, audio and/or visual, to a user that there are no members on a PTT Group being used/monitored by the user and that the user is the only user affiliated to that talkgroup.
14	The PTT Service SHALL, upon request of a User, make available the list of affiliated members on a PTT Group.
15	The PTT Service SHALL provide, upon request, the complete list of members of a PTT Group to an authorized UE.
16	The PTT Service SHALL provide a mechanism to prioritize, dynamically and in real-time, PTT Groups.
17	The PTT Service SHALL provide a mechanism to organize PTT Groups into a hierarchy for prioritization.
Table 2	**Table 2. PTT Private Call Requirements**
1	The PTT Service SHALL provide a means by which a UE can make a 1-to-1 PTT transmission to any user for which it is authorized.
2	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator/Supervisor to configure which users, within their authority, can place a PTT Private Call.
3	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to configure which UEs, within their authority, can place a PTT Private Call to other UEs within the same authority.
4	The PTT Service SHOULD provide an availability check for PTT Private Calls.
5	The PTT Service SHALL provide a mechanism for a PTT Private Call callback request.
6	The PTT Service SHALL provide a UE receiving a PTT Private Call callback request with an indication of which user called and when.
Table 3	**Table 3. PTT Announcement Group Call Requirements**
1	The PTT Service SHALL support Announcement Group Calls in accordance with agency policy [41] as determined by the Public Safety Entity Administrator.
2	The PTT Service SHALL support Announcement Group Calls to a defined geographic area.
3	The PTT Service SHALL allow real-time, dynamic creation and management of Announcement Group Calls by an authorized Public Safety Entity Administrator.
Table 4	**Table 4. PTT Call General Requirements**

[39] Further studies are needed to quantify field length.

[40] Users need to have the ability to consistently implement their own talkgroup aliases in a manner consistent with other agencies within their community.

[41] Policy could include geographic area, site, agency based, discipline based, and role.

1	The PTT Service SHALL provide a mechanism to accommodate ongoing Encoder/Decoder (codec) improvements within LTE. [42]
2	The PTT Service SHALL provide public safety grade service to all members of a PTT Group transmission regardless of group size and/or user density.
3	The PTT Service SHALL provide public safety grade call setup times [43] between any two UEs within coverage of the NPSBN.
4	The PTT Service SHALL provide public safety grade mouth-to-ear latency [44] between any two UEs within coverage of the NPSBN.
5	The PTT Service SHALL provide public safety grade initial lost audio on the NPSBN.
6	The PTT Service SHALL provide public safety grade audio quality or better under public safety operating conditions.
Table 5	**Table 5. PTT Late Call Entry Requirements**
1	The PTT Service SHALL support late call entry.
	The PTT Service SHALL provide Talker IDs to UEs that enter a call late.
	The PTT Service SHALL provide location information to UEs that are late entering a call in progress.
Table 6	**Table 6. PTT Dynamic Group Management Requirements**
1	The PTT Service SHALL provide a mechanism for dynamic creation and termination for PTT Group "patching" by Public Safety Entity Administrators and/or authorized users.
2	The PTT service SHALL provide a mechanism to notify patch PTT Group members of initiation and termination of their PTT Group patch.
3	The PTT service SHALL provide a mechanism to encrypt patched PTT Group transmissions.
Table 7	**Table 7. PTT Call Monitoring Requirements**
1	The PTT Service SHALL allow a UE to actively participate in one PTT Group while simultaneously monitoring additional PTT Groups.
2	The PTT Service SHALL provide a mechanism for an authorized UE to prioritize the order in which multiple PTT Groups are monitored by the UE.
3	The PTT Service SHALL, provide multiple Talker IDs for display on UEs when multiple PTT Groups are monitored.
4	The PTT Service SHOULD provide a mechanism for a Public Safety Entity Administrator and/or authorized user to order the PTT Groups being monitored by the UE.
5	The PTT Service SHALL provide a mechanism for a number (N) of calls to be simultaneously received by a UE, authorized by a Public Safety Entity Administrator, and/or authorized user.
6	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to limit the total number of PTT Group transmission that a UE can simultaneously receive.

[42] This will ensure improvements will be available to users while retaining backwards compatibility to previous versions of the LTE standard.

[43] May be multiple values at different levels of government and geography.

[44] May be multiple values at different levels of government and geography.

7	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to monitor calls to and from PTT Group members within their authority without noticeable impact or knowledge of the user. [45]
8	The PTT Service SHALL provide a mechanism for a PTT Private Call callback request. [46]
9	The PTT Service SHALL provide a UE receiving a PTT Private Call callback request with an indication of which user called and when. [47]
10	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator and/or authorized user to initiate unit monitoring (UE) for UEs within their authority.
11	The PTT Service SHALL provide a mechanism for a Public Safety Entity to record all PTT Group transmissions (including call audio, talker ID, talkpath ID, location of initiating party, and potentially other META data) by their organization.
12	The PTT Service SHALL provide a mechanism to deliver encrypted PTT Group transmissions to a recording interface.
Table 8	**Table 8. PTT Call Priority Requirements**
1	The PTT Service SHALL support ruthless pre-emption.
2	The PTT Service SHALL support top of queue priority.
3	The PTT Service SHALL support a number (N) of users at the top of the priority queue, within an agency's priority levels.
4	The PTT Service SHALL ensure that immediate peril cannot pre-empt emergency calls.
5	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to establish the priority and characteristics of PTT Group transmissions within their jurisdictional authority.
6	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to configure a live time in queue for "top of queue" capability.
7	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to create, under his authority, a pre-emption hierarchy for PTT Group transmissions and their associated users within their jurisdictional authority to promote local management of the service and its resources.
Table 9	**Table 9. PTT Emergency/Imminent Peril Call Requirements**
1	The PTT Service SHALL support emergency calls.
2	The PTT Service SHALL support immediate peril calls.
3	The PTT Service SHALL ensure that emergency and immediate peril calls have the highest priority over all other PTT Group transmissions.
4	The PTT Service SHALL provide a mechanism to ensure that emergency and immediate peril calls, including their content and signaling, have pre-emptive priority over all other types of PTT Group transmissions.
5	The PTT Service SHALL support emergency calls that persist until being acknowledged and terminated based on criteria created by a Public Safety Entity Administrator.

[45] These capabilities need to be defined at the local agency level.
[46] The requirement is the same as requirement #5 in Table 2.
[47] The requirement is the same as requirement #6 in Table 2.

Table 10	**Table 10. PTT Talker ID Requirements**
1	The PTT Service SHALL provide a mechanism such that each PTT Group member has a unique Talker ID.
2	The PTT Service SHALL ensure that each Talker ID has an Alias ID assigned by a Public Safety Entity Administrator and/or authorized user.
3	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator to configure Alias IDs.
4	All UEs SHALL provide a configurable capability to display the Talker ID, PTT Group, Alias ID, and Public Safety Entity name.
5	The PTT Service SHALL provide talker ID.
6	The PTT Service SHALL provide a mechanism for the Talker ID of a user to be associated with that user's authentication and use of the NPSBN. [48]
Table 11	**Table 11. PTT Personality Management Requirements**
1	The PTT Service SHALL provide a mechanism for near real-time UE PTT configuration by a Public Safety Entity Administrator and/or authorized user of PTT Group members.
2	The PTT Service SHALL provide a mechanism for a Public Safety Entity Administrator and/or authorized user to perform personality programming within their authority.
Table 12	**Table 12. PTT Security Requirements**
1	The PTT Service SHALL employ compliant open standards for encryption and authentication, subject to applicable national policy.
2	The PTT Service SHALL provide a mechanism to encrypt all PTT Group transmissions, both user and control plane data (for example, audio, Talker ID, etc.).
3	A UE SHALL provide a mechanism for an authorized user to select what services are available on the UE PRIOR TO full authentication on the UE (for example, 911 calls on commercial UEs).
4	The PTT Service SHALL provide a mechanism to accommodate ongoing security algorithm improvements, which could include over the air key management.
Table 13	**Table 13. PTT Location Requirements**
1	The PTT Service SHALL provide a mechanism for Public Safety Entity Administrators to manage the privacy of location information for users within their authority.
2	The PTT Service SHALL provide a mechanism for an authorized user to prevent location information (for its own UE or another UE) from being conveyed by the PTT Service.
3	The PTT service SHALL provide Talker Location.
Table 14	**Table 14. PTT LTE to P25 Interoperability Requirements**

[48] For example, if a user UE was used on first shift by User A, the Talker ID should be that of the user per their authentication sign on. Another user that utilizes that same device on second shift would have their Talker ID displayed per their authentication sign on.

1	The PTT Service SHALL support fully featured interoperable 1:1 calls between P25 LMR (Trunked and Conventional) subscribers and dispatchers and NPSBN fixed and mobile PTT subscribers and dispatchers.
2	The PTT Service SHALL support fully featured interoperable group calls between P25 LMR (Trunked and Conventional) subscribers and dispatchers and NPSBN fixed and mobile PTT subscribers and dispatchers.
3	The PTT Service SHALL support losing audio and unstoppable transmissions from P25 LMR (Trunked and Conventional) subscribers and dispatchers.
Table 15	**Table 15. PTT LTE to Legacy LMR Interoperability Requirements**
1	The PTT Service SHALL support PTT Private Calls between Legacy LMR subscribers and dispatchers and NPSBN authorized users and dispatchers.
2	The PTT Service SHALL support PTT Group transmissions between Legacy LMR subscribers and dispatchers and NPSBN authorized users and dispatchers.
3	The PTT Service SHALL provide a mechanism to reconcile different codecs between Legacy LMR and NPSBN PTT codecs.
Table 16	**Table 16. PTT LTE to any Future LMR Interface Interoperability Requirements**
1	The PTT Service SHALL support PTT Group transmissions between LMR systems and dispatchers and PTT NPSBN authorized users and dispatchers, regardless of the protocol or mode of operation utilized by the interfacing LMR technology.
2	The PTT Service SHALL provide a mechanism to reconcile codec's utilized by any LMR system interface and NPSBN PTT over LTE.
Table 17	**Table 17. PTT Off-Network Communications Operational Requirements**
1	Off-network PTT Communications SHALL not cause interference to on-network operations and on-network operations SHALL not cause interference to off-network operations.
2	On-network operations SHOULD not cause interference to off-network PTT Communications.
3	Off-network PTT Communications SHALL minimize interference to other off-network devices.
4	Public safety users SHALL have off-network PTT Communications, as necessary and authorized, in the complete absence of any fixed infrastructure.
5	Off-network PTT Communications SHALL allow a minimum number of (N) simultaneous off-network PTT Communication transmissions.
6	Off-network PTT Communications SHALL only be available for authorized users.
7	The PTT Service SHALL provide a notification to a user when approaching the edge of the network. [49]
Table 18	**Table 18. PTT Status Requirements of NPSBN User Off-Network Communications**

[49] Could include audible, visual, or vibration notification.

1	A UE SHALL be capable of switching to an off-network PTT Communications mode when detecting an off-network condition.
2	The PTT Service SHALL allow an authorized user to move PTT Groups off network for use with off-network PTT Communications.
3	An authorized user SHALL be capable of switching to an off-network PTT Communications mode.
4	Off-network PTT Communications SHALL provide a range similar to what is offered by current LMR solutions at an outdoor incident scene. [50]
5	Off-network PTT Communications SHALL provide a range similar to what is offered by current LMR solutions between users within a building and users outside of the building. [51]
6	Off-network PTT Communications SHALL support a number of (N) PTT Groups as authorized by the agencies System Administrator. [52]
Table 19	**Table 19. Off-Network Communications UE Functionality Requirements**
1	A UE SHALL be capable of off-network PTT Communications and on-network PTT at the same time.
2	Off-network PTT Communications SHALL provide a mechanism to dynamically create PTT Groups.
3	Off-network PTT Communications SHALL provide a mechanism for a UE to monitor what PTT Groups are active.
4	Off-network PTT Communications SHALL provide a mechanism for a UE to relay off-network PTT Group transmissions from an on-network UE to an off-network UE.
5	Off-network PTT Communications SHALL provide a mechanism for a UE to relay off-network PTT Group transmissions between off-network UEs.
6	A UE SHALL be capable of transmitting its location, if known, to other UEs when operating off-network.
7	A UE SHALL be capable of utilizing off-network PTT communications while still connected to the NPSBN and access required services.
8	A UE SHALL be capable of being connected to the NPSBN and utilizing required network services while operating off-network PTT communications.

[50] There are many ways to provide this capability, including but not limited to higher power UEs or portable infrastructure.

[51] The users within the building may be on different levels/floors and the varying distances within the building.

[52] Breaking with the qualitative nature of this document, the minimum number of PTT Groups that must be supported is a minimum of 20.

APPENDIX A3:
Public Safety Technical Requirements Analysis Chart

Table References: (M) is Mandatory, (O) is Optional, Green Highlight is Working Group consensus, Yellow Highlight is Working Group secondary position.

CATEGORY	#	REQUIREMENT STATEMENT	Is this a FIELD USER DEVICE Requirement?		Is this a DISPATCHER CONSOLE Requirement?		Is this a SYSTEM FEATURE Requirement?		Capability Rating: Existing LMR Functionality?
			M	O	M	O	M	O	
Interop	1	First responders operating on LMR and LTE networks SHALL be able to communicate with each other including while responding to the scene of the incident as well as upon arrival.							Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	First responders operating on LMR and LTE networks can communicate with each other while inside buildings and other structures.							Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	2	Consoles operating on LMR and LTE networks SHALL be able to monitor and participate in the voice communications between the LMR users and LTE users.							Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	First responders operating on the LTE network at the scene of the incident can communicate among themselves on a common talkgroup and can also communicate with first responders using LMR on the same common talkgroup.							Existing LMR to LTE Interoperability Gateway or Hybrid Device

Interop	3	First responders and consoles SHALL have access to multiple LTE talkgroups to coordinate on scene operations and many of these LTE talkgroups will need to be interconnected with LMR talkgroups to support incident operations.								Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	First responders on LMR networks are able to communicate with other first responders using LTE networks via a designated interworking talkgroup while responding to the incident								Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	LTE consoles are able to communicate with first responders who are on both LTE and LMR networks while they are sharing an interconnected talkgroup.								Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	The interconnection between LMR, NPSBN, and other voice systems (including Push To Talk over Cellular) should support multiple talkgroups for law enforcement, fire, and EMS operations.								Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	First responders and consoles should be able to receive and participate in voice communications on interconnected talkgroup from all first responders, regardless of which radio network they are using.								Existing LMR to LTE Interoperability Gateway or Hybrid Device
Interop	B	First responders and consoles should be able to transmit to all users on the interconnected talkgroup, regardless of which radio network is in use.								Existing LMR to LTE Interoperability Gateway or Hybrid Device

Direct Mode	B	3GPP standards state that an LTE radio may sense the absence of, or significant degradation to, the macro network and automatically switch the radio device to Pro Se direct mode communications.									Existing 3GPP Standard
Direct Mode	4	Local configuration settings SHALL determine if the user device switches automatically or if there is an “out of coverage” warning (requiring an associated manual switch to direct mode).									Existing LMR Capability
Direct Mode	5	Local configuration settings SHALL be determine which direct mode LTE talkgroup the user’s device switches to (e.g., a common interoperable LTE talkgroup or a discipline or agency specific LTE talkgroup).									Existing LMR Capability
Direct Mode	6	A first responder SHALL be able to manually set their LTE device to either remain on the macro network or in direct mode.									Existing LMR Capability
Direct Mode	7	A first responder SHALL be able to communicate with personnel who are on either the macro network or operating in direct mode.									Existing LMR Capability (conventional repeater)
Direct Mode	B	A first responder is able to simultaneously receive designated transmissions occurring on the macro network and from nearby devices operating in direct mode.									Existing LMR Capability (conventional repeater)

Direct Mode	B	A first responder using an LMR radio operating in simplex/direct mode is able to communicate with other first responders operating on LTE direct mode (who are in RF proximity of each other). It is recognized that this will require the use of some intermediary technology.							Existing LMR Conventional/Trunked Scan Capability
Direct Mode	8	First responders SHALL be able to communicate with Extended Primary and regular FirstNet users using direct mode (e.g., mass transit supervisor, DOT snow plow, utility worker).							Existing LMR Capability
Direct Mode	B	An authorized first responder is able to transmit a direct mode emergency broadcast message to all public safety users on direct mode within their RF coverage area.							Existing LMR Capability
Direct Mode	9	A direct mode emergency broadcast message SHALL reach all FirstNet users on all LTE direct mode talkgroups within RF range, including Primary, Extended Primary, and Regular FirstNet users.							No corresponding LMR capability
Direct Mode	10	An emergency broadcast message SHALL reach all FirstNet devices in the immediate area on all macro LTE talkgroups providing an alert to Primary Users, Extended Primary Users, and Regular FirstNet users.							Existing LMR "Super Group" capability

Talker ID	11	A nationwide standardized approach to the assignment of LTE Talker ID and LTE Alias ID SHALL be implemented ensure that the displayed information has meaningful context for first responder agencies.									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	A standardized approach to the assignment of Talker ID aliases will be needed to ensure that information displayed on user devices and consoles can be translated in order to identify personnel, including first responders from out of the area.									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	12	LTE devices and consoles SHALL support and display an alias identity that will provide a functional description of the device user with greater detail than is available from the IMEI (LTE device ID) and IMSI (LTE subscriber ID).									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	13	Talker ID of the first responder SHALL be fully supported even if the first responder is transmitting through an LTE relay.									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	14	The Talker ID data stream SHALL identify which device the first responder is using when they communicate (e.g., transmitting from their vehicle LTE device, their portable LTE device, etc.)									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	15	First responders SHALL be able to view the Talker ID Alias that is assigned to their device to verify it is correct.									Existing LMR Radio ID / Radio Alias Configuration

Talker ID	16	First responder devices and consoles SHALL support a display of recent Talker ID alias for devices that have transmitted on their talkgroup.									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	The Talker ID alias functionality for first responders SHALL support the ability for a first responder to be associated with multiple devices (e.g., vehicle device, portable device, tablet device, etc.)									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	The Talker ID alias functionality further needs to identify the specific device that the first responder is using at the time of the transmission.									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	17	The Talker ID and Talker ID Alias data stream SHALL be designed to meet the initial and longer term interface needs of public safety agencies, including translation done by CAD and other networks.									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	18	A default Talker ID Alias SHALL be supported which will identify devices that are not associated with a specific first responder (e.g., a vehicle device where the first responder has not yet signed on). This Alias should, at a minimum, identify the agency assigned to the device, the device type, and any inventory information (e.g., vehicle number).									Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	Talker ID Aliases shall be shared in the following ways:									Existing LMR Radio ID / Radio Alias Configuration

Talker ID	B	The full Talker ID Alias from **LTE** devices is displayed on designated LTE subscriber devices and consoles. [LTE to LTE]								Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	A Talker ID Alias from **LTE** devices is partially displayed on designated LMR subscriber devices and LMR consoles. [LTE to LMR]								Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	The full Push to Talk ID from **LMR** devices is displayed on designated LTE subscriber devices and consoles. [LMR to LTE]								Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	The full Push to Talk ID from LMR devices is displayed on designated LMR subscriber devices and consoles (e.g., current day operation)								Existing LMR Radio ID / Radio Alias Configuration
Talker ID	B	Talker ID data SHALL be provided to the dispatcher and designated public safety users regardless of the radio network they are using.								Existing LMR Radio ID / Radio Alias Configuration
Talker ID	19	Based on local control preferences, Talker ID data SHOULD be available when first responders are interconnected with Extended Primary and Regular FirstNet users.								Existing LMR /PoC Radio ID-Radio Alias Configuration
Talker ID	20	Based on local control preferences, Talker ID data SHOULD be available when first responders are interconnected with users on other external networks (e.g., school security officers).								

Emergency	21	LTE Emergency Call Button functionality SHALL be configurable by the local public safety agency, including automatic reassignment to a dedicated Emergency Talkgroup or having the first responder remain on the selected talkgroup. Those features should be configurable on a talkgroup by talkgroup basis to allow consistent behavior with neighboring agency policies.								Existing LMR Emergency Transmit Button Features
Emergency	22	The LTE Emergency Call Button alert SHALL display similar information that is contained in the Talker ID/Alias ID, including the first responder's assigned ID, their agency, and information on which LTE device triggered the emergency alert.								Existing LMR Emergency Transmit Button Features
Emergency	23	The LTE Emergency Call Button SHALL transmit the data alert to other LTE devices on the same talkgroup, to the console assigned to the LTE Talkgroup, and to the first responder's home agency console (if different). [LTE to LTE]								Existing LMR Emergency Transmit Button Features
Emergency	24	The LTE Emergency Call Button SHALL transmit the data alert to designated LMR subscriber devices operating on the same interworked talkgroup. [LTE to LMR]								Existing LMR Emergency Transmit Button Features

Emergency	B	An LMR Emergency Call Button alert will send the data alert to other LMR radios on the same talkgroup and to their home LMR PSAP console (e.g., current day operation) [LMR to LMR]								Existing LMR Emergency Transmit Button Features
Emergency	25	An LMR Emergency Call Button SHALL transmit a data alert to designated LTE subscriber radios and LTE consoles operating on the same interworked talkgroup. [LMR to LTE]								New Functionality
Emergency	B	Emergency Button alerts will be provided to the dispatcher and designated public safety users, regardless of the radio network they are using.								Existing LMR Emergency Transmit Button Features
Emergency	26	Based on local control preferences, Emergency Call Button alerts SHOULD be available when first responders are interconnected with non-public safety agencies using LTE or LMR networks.								New Functionality
Encrypt	27	First responders and consoles using LMR and LTE interconnected talkgroups SHALL be able to conduct encrypted voice communications.								Existing LMR Encryption Capabilities
Encrypt	28	Designated LMR and LTE interconnected talkgroups SHALL be able to support secure voice and data communication using an “end-to-end” encryption solution.								Existing LMR Encryption Capabilities

Encrypt	29	Designated LMR and LTE interconnected talkgroups SHALL be able to support secure voice and data communications using a transcoded encryption solution.							Existing LMR Encryption Capabilities
Encrypt	30	First responders SHALL not be required to take any special action to encrypt their communications when accessing a designated encryption talkgroup which includes users from an alternate network (e.g., LMR and LTE).							Existing LMR Encryption Capabilities
Encrypt	B	Encryption between LMR and LTE users will occur on appropriately provisioned talkgroups.							Existing LMR Encryption Capabilities
Encrypt	B	Encryption will be supported when either an LMR or LTE user is added to the talkgroup, or during the late entry of either an LMR or LTE user onto an existing encrypted talkgroup.							Existing LMR Encryption Capabilities
Encrypt	31	First responders and consoles SHALL be alerted if an encrypted talkgroup loses its encryption capability.							Existing LMR Encryption Capabilities
Encrypt	B	First responders will be provided with appropriate policy and training to fully understand the operational considerations of using encrypted communications talkgroups.							
Encrypt	32	Local control policies SHALL determine which users and user devices are authorized to access and engage in encrypted communications.							Existing LMR Encryption Capabilities

Encrypt	33	A number of different encryption keys SHALL be available to public safety agencies in order to segregate different groups of encryption users.								Existing LMR Encryption Capabilities
Encrypt	34	Encryption key management for systems and applications used by public safety agencies SHALL be handled by an authorized representative of the local public safety agency or their designee.								Existing LMR Encryption Capabilities
Encrypt	35	Encryption key management for regional, statewide, and nationwide encrypted LTE talkgroups SHALL be managed by a designated coordinating entity.								Existing LMR Encryption Capabilities
Encrypt	36	Public safety agencies SHOULD be able to distribute new or replacement encryption key data (encryption re-keying) with LMR and LTE user interconnected devices without having to physically access the device.								Existing LMR Encryption Capabilities
SCAN	37	First responders SHALL have the ability to monitor multiple LTE talkgroups to maintain situational awareness of the incident, including interworked LMR/LTE talkgroups.								Existing LMR Conventional/Trunked Scan Capability
SCAN	B	First responders will have the ability to monitor audio on interworking talkgroups that support both LMR and LTE.								Existing LMR Conventional/Trunked Scan Capability

SCAN	38	First responders SHALL be able to scan both static interworked talkgroups (which are configured in advance) and dynamic talkgroups (which are created on an as needed basis).								Existing LMR Conventional/Trunked Scan Capability
SCAN	B	First responders can monitor communications from other first responders on interworking talkgroups who are using both LMR and LTE devices.								Existing LMR Conventional/Trunked Scan Capability
SCAN	39	First responders SHALL have the capability to designate a priority talkgroup, which will distinguish the priority talkgroup audio over the radio communications of other talkgroups being received.								Existing LMR priority Scan Capability
SCAN	40	Local control policies SHALL allow the public safety agency to configure the scan features at the time the device is provisioned for use.								Existing LMR priority Scan Capability
SCAN	B	This includes the ability to assign a fixed priority talkgroup or allow the priority talkgroup to be the selected talkgroup on the user device.								Existing LMR priority Scan Capability
SCAN	41	LTE scan capabilities SHALL match existing LMR radio scan features.								
SCAN	42	While scanning, first responders SHALL have the ability to easily transmit on a talkgroup other than the selected/priority talkgroup.								Existing LMR priority Scan Capability

SCAN	43	First responders using LMR subscriber devices on an LMR/LTE interworked talkgroup SHALL be able to receive sequential scan audio from interworked LTE talkgroups.							New Functionality
Full Duplex	44	LTE consoles SHALL support full duplex voice to permit a telecommunicator to override first responder voice traffic on LTE talkgroups.							Existing LMR Functionality
Full Duplex	45	First responder LTE devices SHALL support full duplex voice conversation with other users on the LTE network.							Existing LTE Functionality
Full Duplex	B	The LTE radio shall support a full duplex voice call that is placed through the Public Switched Telephone Network (PSTN).							Existing LMR Phone Patch or Individual Call
Full Duplex	B	LTE full duplex voice may also exist as a video conference call vs. a full duplex voice only call.							
Full Duplex	46	Specialized LMR and LTE interconnected talkgroups SHOULD support full duplex voice conversation where technically possible.							Existing LMR Phone Patch or Individual Call
Features	B	Specialty devices and consoles will have unique requirements that are not addressed in this use case.							
Features	B	An LTE dispatch console will require unique configurations and features to manage a large number of talkgroups.							Existing LMR Functionality

Features	B	An Incident Commander console (typically a larger wireless device in a supervisory vehicle) will have unique requirements. These may include the need to support multiple independent speakers to spatially manage incoming audio from multiple talkgroups.								Existing LMR Functionality
Features	B	Specialty devices and consoles should support audio record and play back functionality to help manage multiple audio streams.								Existing LMR Functionality

APPENDIX B: Public Safety Requirements Use Cases

These use cases are designed to articulate a basic interworking between public safety agencies which are operating on different technology platforms. It is anticipated that the migration from public safety LMR systems to LTE Mission Critical Voice systems will occur over an extended period of time. From an operational perspective, public safety agencies will have a need to communicate with other first responders who may be operating on a different technology platform.

A city police department may be operating on an LTE based MCPTT system while the adjoining city police department is continuing to operate on an LMR public safety network. Both agencies continue to need fully interoperable communications to support joint activities at the scene of an emergency incident. In another case, a city police department operating on MCPTT continues to need interoperable communications with their local fire department and EMS provider – who may each be on a different transition timeline.

The use cases contained in this report demonstrate some of the capabilities and features that are needed by public safety, specifically targeting existing LMR capabilities that are needed to extend to the LTE solution. These use cases focus on Mission Critical Voice capabilities, including those data features associated with the voice communications network. These use cases do not focus on other technology and data solutions that may also be used at the scene of an incident (e.g., sensors, cameras, etc.).

It should be noted that an initial set of Mission Critical Voice Push to Talk requirements have already been identified by public safety and incorporated into 3GPP standards. They include:

1. Direct Mode/Talk-Around
2. Push to Talk voice
3. Full Duplex Voice
4. Group Call
5. Talker Identification
6. Emergency Alerting
7. Voice Quality

It is expected that the interconnection between LMR and LTE will support dual flow of these features across both systems.

It is not the intent of these use cases to identify all of the features and capabilities that are needed by public safety agencies.

USE CASE 1: Single Talkgroup PTT Voice Interworking

A. Use Case Focus

- Communication between an LMR and LTE officer while responding to the scene of an incident.
- Communications between an LMR and LTE officer while at the scene of an incident.
- Communications between LTE dispatcher and LTE officers on a shared talkgroup.
- Communications between LTE dispatcher and officer using the LMR radio system.

B. Preconditions/Assumptions

- This is a stationary incident with all units operating on their home radio network.
- This use case is based on a **P25 LMR Trunked** radio system interconnected with Mission Critical Voice over LTE.
- Deputy Reddish is a K9 officer with the County Sheriff's Office and is using an LMR radio System
- Officer Lansing is a patrol officer with the City police department which is using an **LTE PTT system**.

C. Use Case Scenario

Officer Lansing is dispatched to a silent burglary alarm at a jewelry store at 2:00 a.m. on a Monday night. Officer Lansing arrives to find the rear door to the business open and requests additional officers to assist him. Additional officers from the same agency arrive and establish a perimeter around the jewelry store, using their LTE MCPTT to communicate between themselves and the dispatcher to coordinate operations.

Officer Lansing requests that the dispatcher call a K9 unit from the Sheriff's Office to come search the building. The City PSAP dispatcher calls the Sheriff's Office PSAP to make the request and then confirms to Officer Lansing that the deputy and K9 are responding. Deputy Reddish, the responding K9 officer, needs to communicate with Officer Lansing on the status of the call

Deputy Reddish arrives at the incident scene and is briefed by Officer Lansing during a face-to--face meeting. Deputy Reddish releases his K9 to search the store. Deputy Reddish's K9 signals that a suspect is cornered in the building. Deputy Reddish and Officer Lansing enter the building to investigate. Both officers are communicating via radio while inside the building.

The officers find Deputy Reddish and Office Lansing struggling with the suspect and assist with his arrest.

D. Public Safety Requirements Discussion

1. The LMR user and the LTE user can communicate with each other while the LMR user is responding to the scene of the incident as well as upon his arrival.
2. The LMR user and the LTE user can communicate with each other inside the building.
3. The LTE dispatcher is able to monitor and participate in the voice communications between the LMR user and the LTE user.
4. The other LTE users at the scene of the incident can communicate among themselves on a common talkgroup and can also communicate with the LMR user on the same common talkgroup.

USE CASE 2: Multi-Talkgroup PTT Voice Interworking

A. Use Case Focus

- The need for multiple interconnected LMR/LTE talkgroups.

B. Preconditions/Assumptions

- This use case is based on a **P25 LMR Trunked** radio system interconnected with Mission Critical Voice over LTE.
- The Lake Town East (LTE) Fire Department is operating on an LTE PTT system.
- The Lower Mountain Regional (LMR) Fire Department is operating on a P25 trunked radio system with access to analog and P25 digital conventional channels.
- Both agencies are operating within the footprint of their respective radio networks.
- Capabilities and requirements identified in previous use cases are not always duplicated in each new use case. Talk ID and Emergency Alert activation were covered in Use Case 1 and are not duplicated in this use case.

C. Use Case Scenario

The Lake Town East Fire Department is dispatched to a report of a building fire in an apartment complex. Three engines arrive to find several cars on fire in an underground parking garage. Thick smoke has risen into the building requiring all floors of the apartment complex to be evacuated. Several residents are suffering from smoke inhalation and are in need of medical treatment.

The Lake Town East battalion chief establishes an Incident Command System and assigns incoming firefighters to separate operational groups, including “fire attack,” “evacuation,” and “medical operations.” Each operational team uses a separate LTE talkgroup to coordinate their actions. There are also additional LTE talkgroups to support communications between the group leaders and the Incident Commander. The fire is spreading to additional vehicles in the underground garage and the Lake Town East Incident Commander requests mutual aid assistance from the nearby Lower Mountain Regional Fire Department.

The Lake Town East Fire Department dispatcher contacts the Lower Mountain Regional Fire Department dispatcher to request assistance. The two dispatchers review available options to provide communications interoperability and select an appropriate solution that will allow the units from both agencies to initially communicate[53] while responding to the incident.

Lower Mountain Regional fire units are now responding to the incident and need to communicate with the Lake Town East battalion chief to receive an update on the fire conditions, to confirm the best approach path, and to identify the staging location. Each incoming fire engine will be assigned to support one of the existing operational groups.

The Lake Town East Fire Department has assigned an officer to manage the staging area to physically meet incoming mutual aid engines. The Incident Commander and the staging officer communicate between

[53] These use cases do not prescribe any technology solution, which may include the use of a common talkgroup, a console or IP patch, or other implementation. Any language that suggests a particular solution is accidental.

themselves on an LTE talkgroup to exchange information on how many engines have arrived and are ready to be assigned. The Incident Commander directs the staging officer to assign each engine to assist a specific group. The staging officer communicates face-to-face with each Lower Mountain Regional fire unit (as they arrive) and provides information on where they should report. This includes the specific location in the building, to what officer they will be assisting/reporting, and what LTE talkgroup is being used for that specific group.

Lower Mountain Regional fire engine 161 arrives first and has been assigned to assist with the evacuation of the apartment complex. Engine 161's crew will work with the firefighters handling the evacuation and will need their LMR portable radios to communicate on the designated LTE talkgroup being used for the evacuation. This assignment is given by the staging officer to the Lake Town East LTE dispatcher who then enables the interworking solution.[54] This may require the Lower Mountain Regional fire units switch to a specific talkgroup on their LMR radio system which is then inter-connected to the appropriate LTE talkgroup being used by the Lake Town East firefighters handling the evacuation.

An agency safety procedure requires a roll call be conducted every 20 minutes to account for all firefighters assigned to the fire attack group. Each firefighter must respond when called and report their location, assignment, and that they are OK. The Lake Town East Incident Commander will conduct this roll call [55] and firefighters operating on both the LTE and LMR radio networks must respond.

When the incident response has been completed, each team of firefighters checks in with the Incident Commander to report that they are leaving the scene and that they are returning to their agency designated radio network/talkgroup.

D. Public Safety Requirements Discussion

1. The LTE public safety agency shall have access to multiple LTE talkgroups to coordinate on scene operations and many of these LTE talkgroups will need to be interconnected with LMR talkgroups to support incident operations.
2. The LMR agency units shall be capable of communicating with the LTE agency units on a designated interworking talkgroup while responding to the incident.[56]
3. The LTE dispatcher shall be able to communicate with users who are using both LTE and LMR devices when they are sharing an interconnected talkgroup.[57]

[54] The interworking solution could also be activated in a number of other ways. This statement is not intended to require that the dispatcher be the controller of the interworking technology.
[55] In some agencies, the roll call is conducted by the fire dispatcher.
[56] This requirement speaks to the need for a wide area solution for interworking vs. a localized solution used at the scene of the incident.
[57] There is no requirement in this use case for the LTE dispatcher to communicate with LMR radios that are not interconnected with the LTE system. This would likely be handled using conventional interoperability radio resources available on the LTE dispatcher's console.

USE CASE 3: Dual On-Network Off-Network PTT Voice

A. Use Case Focus

- The need for interoperable communications between first responders who may be off network.
  - The need for communications between off network LMR users and on network LTE users.
  - The need for communications between off network LTE users and on network LTE users.
  - The need for communications between off network LMR users and off network LTE users.

B. Preconditions/Assumptions

- The Lake Tahoe (LT) Fire Department is operating on an LTE PTT system.
  The Lake Monroe (LM) Fire Department is operating on a P25 trunked radio system with access to analog and P25 digital conventional channels.
- The Lake Tahoe Fire Department is in the coverage area of their LTE network but macro coverage does not reach into the building under construction.
- The Lake Monroe Fire Department units have responded outside the coverage area of their P25 trunked radio network.
- An LTE deployable system is not available to extend communications into the building.
- Capabilities and requirements identified in previous use cases are not always duplicated in each new use case.

C. Use Case Scenario

The Lake Tahoe Fire Department has arrived at an incident in which a worker has fallen into the elevator shaft of a large commercial building that is under construction. The worker is at the base of the elevator shaft which is on the 4^{th} level of an underground parking garage and is severely injured.

Lake Tahoe firefighters and paramedics enter the building and reach the ground floor opening for the elevator shaft. Coverage from the LTE macro network is poor in this area and first responder radio devices are switching between “network” and “ProSe” direct mode. Personnel manually switch their devices to stay on ProSe mode in order to communicate effectively with all members of the rescue team. The lieutenant in charge of the rescue team moves to a position in the building where his LTE device has reliable macro network connectivity.

The lieutenant is able to communicate with the Incident Commander and the dispatcher using the macro network while also being able to communicate with the rescue team that is operating in ProSe mode.[58]

It is quickly determined that assistance will be needed from the Lake Monroe Fire Department's Technical Rescue Team. This need is passed from the rescue team to the lieutenant (using ProSe) and on to the Incident Commander (via the macro network) who places the official request with the dispatcher.[59]

The Lake Monroe Fire Department units begin their response to Lake Tahoe and soon leave the coverage area of their P25 radio network. The units switch to a regional interoperability channel to maintain communications with their dispatcher and with the Lake Tahoe dispatcher.[60]

Lake Monroe fire units arrive on scene and check in with the Incident Commander to receive instructions. They then unpack their technical rescue gear at the ground level elevator shaft. The technical rescue team uses a simplex LMR radio channel to maintain communications between themselves. The technical rescue team leader (using LMR simplex) will also need to communicate directly with the Incident commander (using the macro LTE network).

The technical rescue team uses ropes to lower two firefighter/paramedics down four floors to the bottom of the elevator pit in order to reach the injured employee. The rescue team at the bottom of the elevator pit (using LMR radios) needs to communicate with firefighters at the ground level (who are using LTE radios.)[61]

The firefighter/paramedic determines that the patient needs an IV and a dose of morphine to reduce the pain from several broken bones. The paramedic needs to consult with an emergency room physician to receive permission to administer the drugs. To accomplish this, the firefighters' LMR radio will need to interconnect with an RF network in order to communicate with the hospital.[62]

---

[58] These use cases do not prescribe any technology solution, which may include the use of a common talkgroup, a console, or IP patch or other implementation. Any language that suggests a particular solution is accidental.

[59] It is recognized that some type of intermediary technology may be needed to support this requirement.

[60] This regional interoperability channel is likely an FM analog frequency, and could be a conventional repeater or a simplex base station.

[61] While not ideal, this communication could occur using the LMR simplex radio channel and having personnel at the top of the elevator shaft relay the message to another firefighter who would then retransmit the message on an LTE radio to the Incident Commander. It is also possible that the technical rescue team would borrow LTE radios in order to achieve interoperability. For the purpose of this use case, to illustrate the need for LMR and LTE direct mode interoperability, those options were not selected.

[62] The interworking solution could also be achieved via an LMR radio network extender, like a vehicle repeater; or through the use of a portable LMR/LTE gateway type device that was activated at the incident scene.

The removal of the injured worker from the elevator shaft is coordinated by multiple personnel who are using ropes and other equipment. These personnel, operating on both LMR and LTE devices, must be in constant contact with each other to coordinate the safe extraction of the patient.

Technical Discussion

The intent of this use case is to illustrate public safety requirements that are necessary for safe and efficient operations. However, it is important to recognize that there are a multitude of technical parameters that may influence how public safety utilizes the NPSBN.

For example, first responder's LTE devices may be operating in one of the following modes:

- Connected to macro network.
- Connected to a deployable system in standalone mode with no macro network connection.
- Connected to a deployable system that has a backhaul connection to the macro network.
- Using a UE/Network Relay to obtain macro network or deployable coverage.
- In direct mode/ProSe but using network for RF and timing management.
- In direct mode/ProSe, at cell edge with partial network assistance.
- In direct mode/ProSe, with no network assistance.
- Connected via a Wi-Fi or other RF network.

First responders will need to communicate with other personnel who are in their RF proximity regardless of their connection mode.

- A first responder who is on the macro network should be able to communicate with a nearby first responder who is in direct mode/ProSe.
- A first responder who is on direct mode should be able to communicate with a nearby first responder who is connected to the macro network.

To the fullest extent possible, the first responder user experience should be the same as they transition from one mode of connection to another.

- A first responder may arrive at the scene of the incident and be connected to the macro network.
- As the first responder enters the building their coverage may switch from the macro network to a vehicle-based deployable network solution.
- As the first responder continues to the basement level of the building, their coverage may switch to ProSe.

Each of these modes may provide a different level of functionality for the first responder. Public safety agencies will need to determine whether it is more important to establish a common user experience across these different modes. This may involve selecting a common set of features that are present during all connection types. A common user experience would minimize the need for first responders to learn unique operational characteristics based on how they were connected to the NPSBN.

D. Public Safety Requirements Discussion

1. 3GPP standards state that an LTE radio will sense the absence of, or significant degradation to, the macro network and automatically switch the radio device to ProSe direct mode communications.
    a. Local configuration settings should be used to determine if the user device switches automatically or if there is an "out of coverage" warning (requiring an associated manual switch to ProSe).
    b. Local configuration settings should be used to determine which direct mode LTE talkgroup the user's device switches to (e.g., a common interoperable LTE talkgroup or a discipline or agency specific LTE talkgroup).
2. A first responder shall be able to manually set the radio to either remain on the macro network or the ProSe direct mode.
3. A first responder shall be able to communicate[63] with personnel who are on either the macro network or operating in ProSe direct mode.
4. A first responder shall be able to simultaneously receive designated transmissions occurring on the macro network and from nearby devices operating in ProSe mode.
5. A first responder using an LMR radio operating in simplex/direct mode shall be able to communicate with other first responders operating on LTE ProSe direct mode (who are in RF proximity of each other). It is recognized that this will require the use of some intermediary technology.
6. First responders should be able to communicate with other authorized agencies using direct mode/ProSe (e.g., mass transit supervisor, DOT snow plow, utility worker).
7. An authorized user shall be able to broadcast an emergency message to all public safety users on direct mode/ProSe in their immediate (RF) coverage area[64].
    a. This emergency broadcast shall reach all public safety users on the designated LTE talkgroup or all public safety users on any LTE direct mode talkgroup.

[63] It is recognized that the ability to communicate with nearby devices when in ProSe/direct mode operation is based on being in the geographic RF coverage of the user device.
[64] 3GPP standards provide for Broadband and User Broadcast calls.

b. This emergency broadband should reach all FirstNet[65] devices in the immediate area providing an alert to mass transit supervisors, DOT personnel, utility personnel, etc.

[65] FirstNet has not finalized the definition of "public safety user" and the intent of this statement is to ensure that all personnel supporting the emergency incident are notified of an urgent message, including a directive to evacuate the building.

USE CASE 4: Full Duplex Voice Consultation

A. Use Case Focus

- The need for full duplex voice communications to support an emergency incident.
- This use case does not specifically impact LMR to LTE Migration or interoperability but is listed in order to account for all required elements on LTE PTT Voice.

B. Preconditions/Assumptions

- The Lake Tahoe Fire Department is in the coverage area of their LTE network but macro coverage does not reach into the building under construction.
- Capabilities and requirements identified in previous use cases are not always duplicated in each new use case.

C. Use Case Scenario

The Lake Tahoe Fire Department has arrived at an incident in which a worker has fallen into the elevator shaft of a large commercial building that is under construction. The injured patient has been rescued from the building and has now been placed on a stretcher and loaded into the EMS transport vehicle.

The physician in the trauma center has requested a conference call with the paramedic to further discuss the case. The paramedic uses his public safety LTE device to place a voice call to the physician. The paramedic and the physician engage in a full duplex voice conversation to simultaneously discuss the patient's vital signs, injuries, and treatment plan. The use of full duplex voice allows the paramedic to communicate in a "hands free" mode while they are using their hands to manage patient care.

D. Public Safety Requirements Discussion

1. The LTE radio shall support a full duplex voice conversation using the LTE network to connect to other users.
2. The LTE radio shall support a full duplex voice call that is placed through the Public Switched Telephone Network (PSTN).
3. The LTE full duplex consultation may also take place as a video conference call vs. a full duplex voice only call.
4. LMR and LTE interconnected talkgroups may optionally support full duplex voice conversation.[66]

[66] Full duplex voice between LMR and LTE users would only be possible if the LMR network and LMR device supported full duplex voice

USE CASE 5: PTT Voice Talkgroup Monitor/Scan

A. Use Case Focus

- Functionality of a standard LTE public safety subscriber device (vs. specialty devices and dispatch consoles).
- The need to monitor several talkgroups simultaneously.
- The need for some audio to be prioritized over other audio streams.

B. Preconditions/Assumptions

- This use case is based on a P25 LMR Trunked radio system interconnected with Mission Critical Voice over LTE.
- The Lake Town East (LTE) Fire Department is operating on an LTE PTT system.
- The Lower Mountain Regional (LMR) Fire Department is operating on a P25 trunked radio system with access to analog and P25 digital conventional channels.
- Both agencies are operating within the footprint of their respective radio networks.
- Capabilities and requirements identified in previous use cases are not always duplicated in each new use case.

C. Use Case Scenario

The Lake Town East Fire Department is dispatched to a report of a building fire in an apartment complex. Three engines arrive to find several cars on fire in an underground parking garage. Thick smoke has risen into the building requiring all floors of the apartment complex to be evacuated. Several residents are suffering from smoke inhalation and are in need of medical treatment.

Lower Mountain Regional fire units have responded to provide mutual aid. An LMR to LTE interworking solution has been activated which allows an interconnection between the LMR and LTE talkgroups being used at this incident.

The Lake Town East Incident Commander is using an LTE talkgroup named “Command” for their primary communications. The Incident Commander also needs to simultaneously monitor other interworking talkgroups (which support fire operations involving personnel using both LMR and LTE devices). This allows the Incident Commander to monitor the progress of the firefighters who are attacking the fire in order to verify that conditions are safe enough for continued operations. The Incident Commander’s LTE radio will support the ability to simultaneously receive multiple audio streams. The Incident Commander needs to ensure that voice transmissions on the Command talkgroup are not missed.

D. Public Safety Requirements Discussion

1. The LTE Incident Commander shall have the ability to monitor[67] multiple talkgroups to maintain situational awareness of the incident.
    a. This feature should include the ability to monitor audio on interworking talkgroups that support both LMR and LTE.
    b. This feature should also allow an Incident Commander to monitor LMR talkgroups that may not be an interworked with an LMR/LTE talkgroup.
    c. This capability should include both static interworked talkgroups (which are configured in advance) and dynamic talkgroups (which are created on an as needed basis).
2. The LTE Incident Commander can monitor communications from first responders on interworking talkgroups who are using both LMR and LTE devices.
3. The LTE Incident Commander shall have the capability to designate a priority talkgroup, which will distinguish the priority talkgroup audio over the radio communications of other talkgroups being received.[68]
4. The public safety agency should be able to configure the monitor/scan features at the time the device is provisioned for use.
    a. This includes the ability to assign a fixed priority talkgroup or allow the priority talkgroup to be the selected talkgroup on the user device.
    b. This includes the ability to assign a set of talkgroups to a fixed monitor/scan list or allow the user to create an ad hoc monitor/scan list.
5. The LTE Incident Commander should have the ability to easily transmit on a talkgroup other than the priority talkgroup[69].
6. An Incident Commander operating an LMR subscriber device shall be able to receive sequential scan audio from the interworked LTE talkgroups.[70]
7. Specialty devices and consoles will have unique requirements that are not addressed in this use case.
    a. An LTE dispatch console will require unique configurations and features to manage a large number of talkgroups

[67] This feature is called “scan” in P25 and involves a sequenced channel by channel check for audio. In LTE, the 3GPP standard supports device/network configuration to provide simultaneous reception of audio from more than one talkgroup.

[68] The implementation of this capability may take several forms, including raising the audio level of the priority talkgroup above the audio level of the monitored talkgroups; muting the audio stream of the monitored talkgroups when a transmission is received on the priority talkgroup,

[69] The incident commander may need to quickly answer a radio call coming to them on a monitored talkgroup. A quick transmit capability is desired vs. having the user manually switch their LTE subscriber device to the other talkgroup.

[70] The incident commander using an LMR device on talkgroups that are interworked with LTE talkgroups should experience the same type of scan functionality that they experience today with P25.

b. An Incident Commander console (typically a larger fixed device in a supervisory vehicle) will have unique requirements. These may include the need to support multiple independent speakers to spatially manage incoming audio from multiple talkgroups.
c. Specialty devices and consoles may require audio record and play back functionality to help manage multiple audio streams.

USE CASE 6: Emergency and Unit ID

A. Use Case Focus

- On Network transmission of Unit ID and Emergency Alert.
    - This use case does not address off network capabilities.
- Display of Unit ID information from both LMR and LTE personnel.
- Display of Emergency Alarm activation information for both LMR and LTE personnel.

B. Preconditions/Assumptions

- This use case is based on a **P25 LMR Trunked** radio system interconnected with Mission Critical Voice over LTE.
- The Lake Town East (LTE) Fire Department is operating on an LTE PTT system.
- The Lower Mountain Regional (LMR) Fire Department is operating on a P25 trunked radio system with access to analog and P25 digital conventional channels.
- Both agencies are operating within the footprint of their respective radio networks.
- Capabilities and requirements identified in previous use cases are not always duplicated in each new use case.

C. Use Case Scenario

The Lake Town East Fire Department is dispatched to a report of a building fire in an apartment complex. Three engines arrive to find several cars on fire in an underground parking garage. Thick smoke has risen into the building requiring all floors of the apartment complex to be evacuated. Several residents are suffering from smoke inhalation and are in need of medical treatment.

The Lake Town East battalion chief establishes Incident Command and assigns incoming firefighters to separate operational groups. The Lower Mountain Regional Fire Department is dispatched to provide assistance. An interworking solution[71] is enabled to allow interoperability between the LMR and LTE radio system talkgroups.

Some radio transmissions are difficult to understand due to background noise. The Unit ID of the firefighter transmitting is displayed on the Incident Commander's LTE device, allowing the Incident Commander to confirm the identity of the speaker. Several firefighters have radioed the Incident Commander providing updates on the smoke condition in their specific sections of the building. The Incident Commander needs to confirm information provided by a firefighter who communicated early in the exchange of messages. The Incident Commander is able to scroll through a list of recent Push to Talk IDs.

[71] The interworking solution could also be activated in a number of other ways. This statement is not intended to require that the dispatcher be the controller of the interworking technology.

A firefighter carrying additional hose line to the 3rd floor trips and falls down a set of stairs and is injured. That firefighter activates the Emergency Call button on the LTE device. Information identifying the firefighter is transmitted to designated subscriber radios operating on the interworked talkgroup and to the dispatch consoles.

Discussion

Unit ID provides a significant safety enhancement for public safety agencies. Dispatchers and field personnel can determine which first responder is talking or attempting to transmit. There are frequent situations where immediate assistance is needed but the call for help is not intelligible due to background noise (e.g., a struggle with a suspect) or because the radio is in a poor coverage area.

Public safety radios are seldom used in a fixed assignment. Portable radios may be shared between multiple personnel. Mobile radios in police cars and fire trucks are swapped out by support personnel for maintenance and repair. Some radios are assigned to a function (e.g., Engine 31 company officer) while others are assigned to a specific individual (e.g., a radio assigned to Officer James Taylor).

Some radios may contain multiple Radio IDs based on the number of radio personalities (or separate radio systems) that the device is authorized to communicate with.

Public safety agencies in some regions are working collaboratively to assign unique ranges of Radio ID numbers to each agency or system in an attempt to minimize disruptions when duplicate ID numbers are assigned.

Radio ID is also the cornerstone for the Emergency Call Button feature in which a first responder may request immediate assistance.

Public safety currently uses a variety of approaches and methods in managing Unit IDs on existing LMR systems:

- Display of Unit ID is controlled by the LMR system administrator who can determine which devices and consoles receive PTT IDs.
- Some agencies transmit the basic Radio ID number and require dispatchers to look up the fixed assignment of the device in a spreadsheet or online resource.
- Some agencies program an alias identity into the network that will translate the Radio ID into a more coherent identity (e.g., translate Radio ID 700012345 to “Engine 36” or “Patrol 203”).
- Some agencies interface their LMR radio network and their CAD systems and provide dynamic ID translation:

    - Officers sign into their CAD system Mobile Data Client with their CAD system ID (1Adam12) and also enter their badge number (#1234) and their vehicle number (V610).
    - Radio ID assignment tables then create a real-time translation of the various radio devices used by the officer. If the officer keys up their mobile radio, the incoming Radio ID for the mobile radio is converted to the officer's CAD Unit ID and "1Adam12" is displayed to the dispatcher.
- Some LMR systems (non P25) allow for alias ID to be transmitted over the air. This includes MDC1200 signaling as well as DMR and NexEdge. Some systems support a static (fixed) alias and other systems dynamically assign an alias based on a subscriber log in.

In the NPSBN environment a single nationwide network will be created. This will allow a much greater range of interoperability between first responders units and devices. The system will need to support the provision of meaningful IDs for all users, including out of area users. For example, a state trooper who is traveling to a training session more than 100 miles from their home base needs to contact a local Sheriff's Office to request assistance. The Unit ID of the trooper should be sufficiently detailed to allow the public safety agency receiving his transmissions to realize his agency affiliation and personal identity.

The ability to interoperate with secondary responder agencies will also require Radio ID coordination. Transportation, public works, and other units may be supporting a major incident and need to communicate with first responders. The exchange of Unit IDs should allow a user to determine the identity of the agency they are communicating with and the identity of the specific unit within that agency.

First responders may use multiple devices during their duty shift. A police officer may use a vehicle-based LTE radio, a portable LTE radio, and an LTE tablet. All of the devices will need to identify the officer as the "user" and further identify which device the officer is using at that instance.

From an LMR to LTE migration perspective, it appears that LTE will support a more robust Unit ID than P25, (with the potential for more characters and information). Radio ID (and Emergency Call Button data) will need to traverse between LMR and LTE systems. It is likely that a full LTE Radio ID may need to be translated into an ID that can be supported by a P25 subscriber device or console.

LTE supports a number of device and service identifiers including IMEI (used by the carrier for provisioning), IMSI (used by the carrier for certain service aspects), and the SIM card. 3GPP standards also support a MCPTT ID and alias ID. In this context, "Talker ID" is meant to identify the first responder for public safety purposes (e.g., Officer Badge number #9999, the CAD Radio

Call Sign "1Adam12," and the alias of a device not associated with a first responder (e.g., Seattle PD Vehicle #1234).

D. Public Safety Requirements Discussion – Talker ID[72]

1. A standardized approach to the assignment of Talker ID will be needed to manage a nationwide network of devices.
2. A standardized approach to the assignment of Talker ID aliases will be needed to ensure that displayed information has meaningful context for first responder agencies.
3. LTE devices shall support an alias identity that will provide a functional description of the device user with greater detail than is available from the IMEI (LTE device ID) and IMSI (LTE subscriber ID).
4. Talker ID of the first responder shall be fully supported even if the first responder is transmitting through an LTE relay.
5. Talker ID shall also identify which device the first responder is using when they communicate (e.g., transmitting from their vehicle LTE device, their portable LTE device, etc.)
6. First responders shall be able to view the Talker ID Alias that is assigned to their device to verify it is correct.
7. First responders shall be able to view a list of prior Talker ID alias displaying others who have recently transmitted on their talkgroup.
8. The Talker ID alias functionality for first responders must support the ability for a single first responder to be associated with multiple devices.[73] The Talker ID alias functionality further needs to identify the specific device that the first responder is using at the time of the transmission.
9. Several Talker ID alias translation options shall be available to meet the initial and longer term interface needs of public safety agencies.[74]
10. A default Talker ID Alias shall be provided which will identify devices which have not yet been signed into by a first responder.[75]
11. Talker ID Aliases shall be shared in the following ways:

[72] Talker ID refers generally to the identification of the first responder or a device that is transmitting. This may be an alias ID or take on some other form. MCID is the Mission Critical ID noted in 3GPP standards.

[73] An individual first responder may use a vehicle-mounted LTE device, a portable LTE device, and an LTE tablet during their assigned shift and each of these devices may be capable of either accessing LTE MCPTT or sending an Emergency Alarm.

[74] First responder agencies today use a variety of LMR Radio ID translation interfaces which will need to be supported during the migration to LTE.

[75] LMR radio devices today may be used in an emergency by a first responder who is not on duty and is therefore not logged in to the CAD system. Public Safety agencies shall be able to identify devices in use which are not associated with a first responder, either to assist them in an emergency or to detect lost and stolen equipment, if those devices are able to transmit or send an Emergency signal under those conditions

a) The full Talker ID Alias from **LTE** devices is displayed on designated LTE subscriber devices and consoles.
b) A Talker ID Alias from **LTE** devices is partially displayed on designated LMR subscriber devices and LMR consoles.
c) The full Push to Talk ID from **LMR** devices is displayed on designated LTE subscriber devices and consoles.
d) The full Push to Talk ID from LMR devices is displayed on designated LMR subscriber devices and consoles (e.g., current day operation)

E. Public Safety Requirements Discussion – Emergency Call Button

1. The Emergency Call Button behavior shall be configurable by the local agency, including automatic reassignment to a dedicated Emergency TalkGroup or having the first responder remain on the selected talkgroup. Those features should be configurable on a talkgroup by talkgroup basis to allow consistent behavior with neighboring agency policies.
2. The LTE data alert shall contain similar information that is contained in the Talker ID, including the identity of the first responder, and from which LTE device the emergency alert originated.
3. The LTE radio emergency call button sends the data alert to other LTE devices on the same talkgroup and to their home LTE PSAP dispatcher console. (LTE to LTE)
4. A portion of the LTE radio emergency alert shall be broadcast and displayed to designated LMR subscriber devices.[76] (LTE to LMR)
5. An Emergency Call Button alert from an LMR radio shall send the data alert to other LMR radios on the same talkgroup and to their home LMR PSAP console (e.g., current day operation) [LMR to LMR]
6. An Emergency Call Button alert from an LMR radio shall send a data alert to designated LTE subscriber radios and LTE consoles. [LMR to LTE]

[76] The incident commander, or other supervising officer at the scene, may be operating an LMR radio. It is recognized that P25 standards will not support the full range of data that might be included in an LTE Talker ID.

USE CASE 7: PTT Interworking LMR, NPSBN and Push to Talk over Cellular (PoC)

Public safety agencies are currently leveraging broadband Push to Talk over Cellular (PoC) systems to augment their LMR radio networks. These PoC systems may be interconnected to the public safety LMR systems to provide various levels of interoperability. It will be necessary for these PoC systems to be interconnected with both LMR and NPSBN Push to Talk networks to support public safety. Public safety agencies may also need to interconnect with non first responder agencies (e.g., school security personnel, retail, and business security) that may be using PoC or Over the Top (OtT) Push to Talk voice applications.

A. Use Case Focus:

- Interoperability between LMR, NPSBN, and PoC and OoT users.

B. Preconditions/Assumptions:

- This is a stationary incident with all units operating on their home radio network.
- This use case is based on a **P25 LMR** radio system interconnected with both Mission Critical Voice over LTE (NPSBN) and Broadband PoC service.
    - The Broadband PoC service is likely to be a carrier network provided solution to ensure priority and quality of service vs. an Over the Top (OtT) application.

C. Use Case Scenario

The City of Lone Mountain hosts a large street festival each year that requires hundreds of public safety and support personnel to manage the event. Outside personnel are brought in to supplement the local city resources in providing emergency response, directing traffic, managing crowds, and providing visitor information and services.

All personnel supporting the event need instant group communications with their team to be effective in their role. First responders and support personnel are using several different voice networks, including the City's LMR system, the NPSBN network, and a Push to Talk solution provided by a commercial carrier. All personnel are organized into one of two groups:

- Users who **do not** need direct communications with first responders to complete their duties, such as concessionaires and logistic personnel. However, these personnel do need to be able to communicate directly with first responders in a crisis.

- First responders who **do** need direct communications with law enforcement, fire, EMS, and designated support personnel (e.g., first aid station, traffic posts, security).

Each of the three radio networks has unique channels and talkgroups to support the operations of their users. Several talkgroups have been designated to provide interoperability between

users on the three networks. These talkgroups are interconnected allowing users on any network to communicate with users on the other networks.

The Lone Mountain street festival starts uneventfully. Support personnel communicate with each other to manage administrative and logistical functions. First responders are able to communicate with each other to coordinate incident response.

A visitor collapses at the ticket booth and appears to be having a heart attack. The employee in the ticket booth switches her PoC radio to a designated emergency talkgroup that is interconnected with the LMR, NPSBN, and PoC systems and requests help. Two paramedics on bicycles hear the announcement on their NPSBN devices and respond to the scene. An EMS crew staffing a transport ambulance also hears the announcement on their LMR radio and responds to the scene. The paramedics arrive quickly and use their NPSBN radios to communicate with the ambulance crew using LMR and exchange patient information and directions on the best route to reach the ticket booth.

A police officer, using the LMR system, communicates with security staff on the PoC network to stop traffic so the ambulance can access the scene. A police officer on the LMR system communicates with a sheriff's deputy using the NPSBN to open a locked gate for quicker access.

D. Technical Discussion

The intent of this use case is to illustrate public safety requirements that are necessary for safe and efficient operations. However, it is important to recognize that there are a multitude of technical parameters that may influence how public safety utilizes the NPSBN.

- Technical issues should be fully explored that might negatively impact the operation of a three-way interconnection between LMR, NPSBN and Cellular PTT.
- Operational and policy implications involving the use of a three-way interconnection need to be examined. Who can communicate with whom and under what circumstances?
- There are limitations on the number of simultaneous talk group patches set up using an ISSI gateway (e.g., impact of ISSI licensing)
- There are encryption issues when interconnecting LMR with the NPSBN and a commercial carrier.
- Different features and capabilities may be present when networks are interconnected, resulting in the potential loss of some expected capabilities. This is especially true when patching to a non public safety agency/system. (e.g., would a public safety agency expect Emergency Button activation messages to be shared across the network when working with a shopping mall security officer).

E. Public Safety Requirements Discussion

The requirements for interworked communications between LMR/NPSBN and PoC should be similar to those for LMR/NPSBN.

1. The interconnection between LMR, NPSBN, and PoC should support multiple talkgroups for law enforcement, fire, and EMS operations.
2. Users, including the dispatcher, should be able to receive voice communications on the interconnected talkgroup from all first responders, regardless of which radio network they are using.
3. Users, including the dispatcher, should be able to transmit to all users on the interconnected talkgroup, regardless of which radio network they are using.
4. Talker ID data shall be provided to the dispatcher and designated public safety users regardless of the radio network they are using.
    a. Talker ID data may not be shared between non-public safety agencies[77] who are interconnected (e.g., a school security officer)
5. Emergency Button alerts should be provided to the dispatcher and designated public safety users, regardless of the radio network they are using.
    a. Emergency Button data may not be shared between non public safety agencies[78] who are interconnected (e.g., a school security officer)

[77] It is recognized that sharing of Talker ID information is dependent on the type of radio infrastructure and local configuration settings of the nonpublic safety agency.

[78] It is recognized that sharing of Emergency Button information is dependent on the type of radio infrastructure and local configuration settings of the non-public safety agency.

USE CASE 8: Encryption

This use case is an adaptation of the public safety response described in Use Case #1 involving a burglary in progress (Single Talkgroup PTT Voice Interworking).

Many public safety agencies employ encryption on their Land Mobile Radio systems to prevent unauthorized disclosure of confidential and sensitive information. There are a variety of encryption methodologies, including those which are standards based and others that are proprietary to a specific vendor. A number of other factors influence successful encryption including the use of shared encryption keys and other set up parameters. Public safety agencies using the NPSBN will need to conduct encrypted communications with other first responders operating on LMR networks.

This use case is designed to identify common public safety requirements regarding encryption and voice services. The use case acknowledges a multitude of different technology implementations but does not seek to create unique requirements for these configurations. The first responder needs a consistent user experience that, to the extent possible, is replicated across the different encryption solutions. It is recognized that various solutions provide different levels of security. The U.S. Department of Homeland Security's, Office of Emergency Communications, has recently published reports on technical considerations and best practices for LMR encryption.[79] The Department of Defense also recently published guidelines for use of encryption.[80]

A. Use Case Focus

- Communication between personnel using both LMR and LTE devices.
- Communication between LTE dispatcher and personnel using either LMR or LTE devices.
- Communication between LMR dispatcher and personnel using either LMR or LTE devices.

B. Preconditions/Assumptions

- This is a stationary incident with all units operating on their home radio network.
- This use case is based on a P25 LMR Trunked radio system interconnected with Mission Critical Voice over LTE.
- Deputy Reddish is a K9 officer with the County Sheriff's Office and is using an LMR Radio System

[79] DHS Encryption Reports, https://www.dhs.gov/safecom/blog/2016/10/12/fpic-releases-encryption-documents
[80] DOD Instruction Number 4650.10, Land Mobile Radio (LMR) Interoperability and Standardization, Effective April 13, 2016; http://www.dtic.mil/whs/directives/corres/pdf/465010p.pdf

- Officer Lansing is a patrol officer with the City police department which is using an LTE PTT System.

C. Use Case Scenario

Officer Lansing is dispatched to a silent burglary alarm at a jewelry store at 2:00 a.m. on a Monday night. A team of professional jewelry thieves have been operating in the area and are believed to be using radio scanners to monitor law enforcement channels. Agency personnel have been instructed to utilize the encryption feature on their NPSBN LTE devices.

Officer Lansing arrives to find the rear door to the business open and requests additional officers to assist him. Additional officers from the same agency arrive and establish a perimeter around the jewelry store, using their LTE MCPTT to conduct encrypted communications between themselves and the dispatcher to coordinate operations.

Officer Lansing requests that the dispatcher call a K9 unit from the Sheriff's Office to come search the building. The City PSAP dispatcher calls the Sheriff's Office PSAP to make the request and then confirms to Officer Lansing that the deputy and K9 are responding. Deputy Reddish, the responding K9 officer, is using an LMR radio which is also encrypted. He needs to communicate with Officer Lansing on the status of the call. The City PSAP supervisor enables an interconnection between the LMR talkgroup being used by Deputy Reddish and the LTE talkgroup being used by Officer Lansing.

The City PSAP dispatcher, Deputy Reddish, Officer Lansing, and other city police officers at the incident scene coordinate the response to this incident.

D. NPSTC Working Group Technical Discussion

There is significant technical complexity surrounding the implementation of encryption and those issues become more complex when you interconnect LMR and LTE networks. Appendix "C" provides a detailed description of LMR-LTE interworking issues. The following information provides a high-level overview of the technical issues that would impact this use case.

Types of LMR Encryption: In general, digital voice encryption is either based on standards or is provided by a manufacturer as a proprietary feature. Successful interoperability requires the use of a common encryption type as well as successful provisioning of the subscriber devices.

The currently accepted standard for encryption is the 256-bit "Advanced Encryption Standard," also known as AES. AES is the designated encryption standard for U.S. federal government agencies. A number of vendor proprietary encryption systems are also in use across the United States. These offer varying degrees of message security.

Types of LTE Encryption: LTE encryption functions differently than LMR encryption and can be implemented in different ways depending on the level of message security that is required. There are many technical aspects to LTE encryption at the device, application, and network level. This report will focus on two general approaches to LTE encryption:

- Over the Air Interface encryption only provides secure communications for those portions of the message that are broadcast between the user device and the radio tower.[81] Messages may then traverse the fixed portion of the network without encryption.
- End-to-End encryption occurs at the application layer and maintains the security of the message as it moves from the application on the user's device to other destinations. This is also called "application level encryption.[82]"

Encryption between LMR and LTE Systems

There are two technical approaches to managing encryption of voice communications when LMR and LTE systems are interconnected:

- LMR/LTE Common Encryption: This requires the use of the same encryption and voice coding components on both the LMR and LTE devices, including the encryption algorithm, encryption key, and vocoder. This prevents the need for transcoding between different encryption and vocoder systems.
- LMR/LTE Dissimilar Encryption: This involves the use of one type of digital encryption and vocoder on the LMR network and a different type of encryption and vocoder on the LTE network. When LMR and LTE networks are joined, a decode/recode of the message is necessary at the point of the interconnection. This could produce a security vulnerability if the interconnection point is not properly secured.

LMR/LTE Interconnection and Encryption Issues

Before LMR-LTE encryption can occur, the two networks must be connected. There are different ways to connect LMR and LTE networks and each solution may offer different levels of operational capability. Certain solutions may not support robust encryption. Interconnection of networks may occur at the core network (e.g., the infrastructure level) or may occur in the field using specialized devices (e.g., an IP gateway on a mobile command vehicle).

3GPP is currently defining standards to support LMR and LTE interworking. Their focus is on the LTE side of the interworking solution. Other organizations, including ATIS and TIA, are working to develop standards for the LMR side of the interworking solution.

[81] Known as the eNodeB.

[82] This involves encryption from the user device/client application to the application server.

Existing technologies that interconnect disparate LMR systems will likely be used to achieve interworking between LMR and LTE networks, which will help facilitate encryption.

An LMR-LTE interworking solution involving a P25 radio network may likely leverage a number of existing interface solutions, including the Inter RF Sub-System Interface (ISSI), the Console Sub-System Interface (CSSI), and the Digital Fixed Station Interface (DFSI).

It should be noted that while many agencies use the P25 standard in their LMR radio systems, other public safety agencies use proprietary trunked solutions or operate using legacy conventional radio systems. An LMR-LTE interworking solution for non-P25 networks may require a separate solution to effectively interoperate with LTE. Console patching and other audio gateway solutions are available to interconnect analog and proprietary digital communications networks with other systems.

End-to-end encryption was viewed as the preferred method for a number of operational and technical reasons. This requires the utilization of a common vocoder[83] and common encryption scheme. Two potential solutions[84] were reviewed by the Working Group that would allow end-to-end encryption.

- First responders would be directed to select a specific interoperability talkgroup designated for encryption. The LTE system would be preconfigured so that LTE users are automatically steered to use a P25 vocoder and P25 encryption scheme.
- If a dedicated LMR/LTE encryption talkgroup is not used, then a solution is needed to manage the addition of a P25 LMR user who is being added to an encrypted LTE talkgroup. During call set up, following the arrival of a LMR P25 user, the LTE network can do a negotiation and change the vocoder of the LTE first responders to match the P25 vocoder and encryption scheme.

Other methods of joint LMR-LTE encryption often result in the need to transcode the message as it crosses the network interface. A first responder may be using one type of encryption on their LMR system and need to communicate with another first responder who is using an LTE encryption methodology. Each transmission is decoded from one encryption scheme into a clear message and then re-coded with the encryption scheme of the other network and passed to that user. This is an acceptable technical solution if network security considerations are managed and the implementation meets the operational requirements of the public safety agencies. Any interconnection of LMR and LTE systems requires careful engineering analysis to reduce latency and maximize the performance of message transfer.

These approaches would require several technical components in the interworking solution:

[83] It should be noted that P25 networks use a different vocoder than LTE networks. 3GPP has also identified AMR Wideband as the common vocoder to be used for LTE mission critical voice.
[84] There are a number of different component and configuration options to achieve this result.

- The interworking solution needs to support transcoding in order to manage the use of disparate encryption solutions (where the LMR system and the LTE system are using different encryption solutions).
- The interworking solution needs to be able to provision new keys.
- The interworking solution needs to support the late entry of users: fix
    - Late entry of a P25 user LMR user into an LMR/LTE encrypted talkgroup.
    - Late entry of an LTE user into a P25 LMR/LTE encrypted talkgroup.

The following additional challenges were raised:

- The current 3GPP standard does not support local control of encryption keys. This would presumably require that all aspects of encryption, including key management, would be handled by the NPSBN network operator. This might be viewed as unacceptable to public safety agencies which need to ensure secure communications among authorized users.
- It is recommended that encryption be done at the application level to provide end-to-end continuity of message security.
- If a first responder's LTE device supports encryption and is stolen, it may be necessary to rekey the encryption of all other users to maintain secure communications.85.Encryption keys must also be changed on a regular basis to maintain security of communications. 3GPP has defined encryption key management practices for LTE and P25 has defined encryption key management practices for P25 LMR systems. Additional work is needed to determine how these two standards will interoperate.
- Encryption between a group of first responders who are operating on both the NPSBN and on a Push to Talk over Cellular (POC) network has not been addressed, nor has encryption between first responders operating on NPSBN, POC and LMR simultaneously.[86]
- The use of P25 "multi-key" supports the transition period when a new encryption key is released but not all subscriber devices are yet updated. Tactical voice communications may need to continue during the subscriber device update process. 3GPP standards need to address how this will occur during an LMR/LTE interconnection (where two valid LMR encryption keys are in use.)[87]
- LMR Link Layer encryption. There are several issues relating to voice and data payload encryption including ID translation across the interworking interface. In LMR

[85] While it may be possible to remotely disable the stolen device, some high risk tactical operations would require distribution of a new encryption key.
[86] These issues are being noted in the report, but are considered out of scope for this document.
[87] 3GPP standards do not address multi-key for LTE.

the Device ID and TalkGroup ID are encrypted.[88] Public safety agencies may desire to have these same data elements hidden on the LTE network.

E. Public Safety Requirements

The Working Group identified a number of public safety requirements that are necessary for first responders when using encrypted communications, including LMR to LTE interworked communications.

1. NPSBN users shall be able to conduct voice and data[89] communications using "end-to-end" encryption.
    a. Transcoded encryption is also a viable technical solution.
2. NPSBN users shall be able to conduct encrypted voice communications[90] when speaking to an LMR user on an appropriately provisioned interconnection.[91]
3. The first responder should not be required to take any additional action to access encrypted communications with a user on an alternate network (e.g., LMR and LTE)
    a. This requirement includes communications on appropriately provisioned talkgroups involving LMR and LTE users.
    b. This requirement includes communications on LMR/LTE provisioned talkgroups when either an LMR or LTE user is added to the talkgroup, or during the late entry of either an LMR or LTE user onto an existing encrypted talkgroup.
4. An NPSBN user should be alerted if communications are no longer encrypted.[92]
5. NPSBN users shall be provided with appropriate policy and training to fully understand the operational considerations of using encrypted communications talkgroups.[93]
6. Public safety agencies shall control which users and user devices are authorized to access and engage in encrypted communications.
7. There shall be a number of different encryption keys available to public safety agencies allowing segregation of encryption users. For example, a law enforcement

[88] On LMR, encrypted communications include the device ID and the TalkGroup ID. In a transcoded environment, these data elements have to be exposed at the interworking interface in order to be passed on to the other network. P25 is currently working on this issue.

[89] While this report deals with Mission Critical Voice issues, it is important to note that encryption of all data, including message traffic, video, and application data is necessary

[90] This requirement acknowledges that there are various ways to achieve interoperability between the LMR and LTE encrypted users.

[91] It is recognized that effective interworking of encrypted communications between LMR and LTE networks requires specific configuration settings in both systems.

[92] Loss of encryption could be related to a failure or due to the unexpected interconnection with a non encrypted talkgroup.

[93] This statement is meant to address operational policy which will drive training of first responders. It is not intended to require a full technical briefing on the interworking solution.

SWAT team may use a unique encryption key that is not available to other members of the same agency using encryption.

8. Encryption key management for systems and applications used by public safety agencies shall be handled by an authorized representative of the local public safety agency.
9. Key management for regional, statewide, and nationwide encrypted LTE talkgroups should be managed by a designated coordinating entity.
10. Public safety agencies should be able to share new or replacement encryption key data (encryption re-keying) with LMR and LTE user interconnected devices without having to physically access the device.

APPENDIX C: NPSTC-PSCR Mission Critical Voice Round Table Report[94]

National Public Safety Telecommunications Council
Public Safety Communications Research Program
Mission Critical Voice Task Group Meeting Summary
November 11, 2016

In July and August of 2016, the National Public Safety Telecommunications Council (NPSTC) and the Public Safety Communications Research (PSCR) program brought together a number of public safety and industry representatives to review select Mission Critical Voice functionality. The effort was to ensure that any outstanding issues were addressed sufficiently as they may be the subject of upcoming PSCR Federal Funding Opportunities (FFO) where the implementation of public safety communications and Mission Critical Voice capabilities in a broadband environment will be the subject of contests and prize challenges to identify solutions that support public safety.

A select group of 15 public safety and industry representatives provided additional industry perspective, public safety clarity, and standards bodies' viewpoints on a number of outstanding issues over the course of six conference calls over a period of 2 months. The goal of the effort was to facilitate a deeper discussion on how floor control, direct mode operations (DMO), and discovery features are currently understood to work in today's public safety radio systems as well as how they may work in a broadband Push to Talk (PTT) environment. Additionally, the group highlighted potential value-added components for each area.

As public safety begins to utilize more heavily and more greatly depend on public safety broadband resources for its voice communications, discussion and dialogue need to continue on the optimum configuration of those resources. Some feature sets might need to start being utilized in a rudimentary manner by public safety that may not take full advantage of the technology until the use of new capabilities resulting from those features are familiar enough for public safety use.

The information gathered can impact a number of anticipated services, but all discussions were focused on PTT services and impact to public PTT/voice operations.

[94] The Round Table summary report is included in this Appendix. The complete report is available from NPSTC, which includes the minutes and technical discussion from each meeting.

The following information provides an overview of the discussions that took place in the summer of 2016 that were centered on public safety voice operations exclusively. The full meeting minutes from each conference call are included in the Appendix.

This document is not considered an official report by either NPSTC or PSCR. It is a summary of task group discussions which are now being forwarded to the NPSTC LMR-LTE Integration and Migration Working Group for their deliberation.

Adaptive/Dynamic Floor Control

Today, public safety operates in a PTT environment where override is not generally utilized when accessing talkgroups in an LTE environment, and floor control could evolve to incorporate dynamic prioritization for a user within a talkgroup that was based on their biometrics, situation, conditions, location, etc. Public safety users today seem to work effectively in an environment where group PTT prioritization is generally not used in favor of an environment in which all users are equal in their ability to access the voice resource in a group. This methodology works for public safety users and meets their expectations today.

1. In next generation voice networks, it will be possible for all users to have equal status in the manner in which they access the network, but other factors can contribute to a user's ability to access a voice resource. A number of actions or variables should be able to be "triggered" to elevate a user's priority based on a number of values. Location based services might be integrated into PTT services that will provide location information per PTT and geo-fencing can be utilized to heighten the priority of users within a specific area. For example, with the use of bio-medical sensors placed on a firefighter's body, a firefighter with an unstable heart rate or low blood oxygen level can, via the sensor reading, be *dynamically prioritized* to allow that user access to the network on a prioritized basis at that instant. In another example, a police officer's vest may detect the impact from a bullet with a resulting dynamic increase in priority. The use of sensors associated with a responder will allow for more information to contribute to the needs of the users and the manner in which they access information via the network.

2. Floor control in accordance with PTT voice and prioritization can be enhanced in a broadband environment in a number of different ways. In today's PTT systems, the console operator usually has the ability to override the radio traffic of a specific user in a talkgroup. Options in today's systems allow the overridden radio traffic to continue to be recorded at the console despite the override and allow for the traffic to be retrieved when necessary. This type of PTT priority of resources can be distributed beyond the console operations by agencies seeking to change the priority of its users as needed during incidents based on the user agency's preferences.

3. While public safety's use of today's inter-connected P25 systems might not reflect the need to prioritize users when accessing trunked systems, new capabilities and the ability to dynamically prioritize users based on their operating conditions or their situation might allow the introduction of new capabilities that might enhance the tools that public safety utilizes regularly to complete their mission while keeping them safer at the same time. Thus, a heightened awareness of public safety floor control and how users access voice resources will benefit system administrators and planners in future broadband voice solutions ensuring operational needs are met.

4. Radio discipline and the ability to talk and listen to the radio traffic of other users in an inherent part of public safety communications and critical to the well-being and safety of users in the field. Users in the field who are in a position to assist other users can monitor radio traffic and support their fellow users by monitoring radio traffic. The proper mix of users talking when they need to talk and listening when they need to listen seems to be struck in today's PTT voice environment where users access channels equally and all user levels of PTT priority are the same.

Direct Mode

Direct Mode Operations (DMO) utilized by public safety today allows for off network voice communications between units in the field within range of each other without the assistance of any infrastructure. DMO is an inherent part of public safety operations and will be needed in any future broadband voice solution intended to support public safety's needs.

1. Concurrent on-network/off-network DMO and UE-to-network relay: Public safety seeks to have the capability for their devices to monitor traffic on the macro network they are affiliated with while concurrently being able to monitor radio traffic originating from users operating off of the network. Subsequently, the need for multiple receivers was a topic of discussion within the task group. Several participants of the group are involved in the 3GPP standards development process public safety's and have been able to contribute to the group from the standards perspective. The need for multiple receivers in a device has been identified in the 3GPP standards process and the implementation of those two receivers needs to be in a manner that supports public safety's needs. While it is important for the standards process to establish the technologies and capabilities that can meet public safety's operational needs, often the *implementation* of the elements and attributes developed within the standards process are equally as important as the functionality resulting from the standards themselves.

2. An educational piece comparing and managing expectations between today's voice DMO operations and tomorrow's DMO was identified as necessary to ensure users are aware of the differences between current and future DMO operations and user

needs/expectations are met in any new broadband voice environment. There are too many variables in today's public safety's DMO environment today that will change in future DMO operations to not address the differences in a manner that takes all of these important points into account. A deliverable that addresses DMO operations developed to educate public safety about DMO operations in a broadband network is necessary and appropriate for users anticipating both mission critical use and non-mission critical use. It is absolutely critical users are made aware of DMO operations and how those operations may change in a broadband PTT voice environment.

3. The introduction of new technologies necessitates training and awareness of the capabilities associated with DMO in a broadband environment. A number of elements associated with public safety DMO have yet to be finalized and we encourage public safety input into these discussions. Some of those issues are:
    - How are users notified if they've moved off of the network and enabled with DMO operations?
    - Are users that were in the group that fell off the network's group notified that the user is now off network?
    - If users are moved off network by the network (not by their own doing) where do their devices "land"? Is there an established common, off network talkgroup or channel that any device that left the network would revert to?
    - Should all NPSBN devices be able to provision or activate DMO capabilities? What about secondary users of NPSBN? Is DMO a baseline capability inherent in any NPSBN device or inherent only on any *public safety* NPSBN device?
    - Are there opportunities for off network resources to be re-used within the NPSBN? In adjacent cells, can the network recognize that resource blocks for DMO operations are already used for DMO operations in adjacent cells and allow those blocks to be used for DMO operations in that cell as well? Can the use of those resources be coordinated within the network and between cell sectors?
    - Can users operating in DMO receive "broadcast" messages specifically intended for DMO users? Can a group distribution be specifically designed for DMO uses within a cell sector? Across cell sectors? Is there a mechanism to facilitate alerting to those participating in DMO at a specific site or sites in a larger event?

Discovery

Discovery capabilities can benefit public safety users in discovering other users as well as other devices. Discussions highlighted that the ability for users to discover sensors and relays may be equally as important to public safety as discovery of other users. Public safety's implementation of discovery operations will be a new technology that has no historical applicability so public safety will be cautious in its implementation of discovery applications until their users are comfortable with the technology and the applications the technology creates and enhances.

In addition, the introduction of the ProSe 'discovery' process in commercial wireless technologies is a new feature for public safety communications to develop and, while there is great hope that discovery capabilities will be contributable to public safety operations, the specific applications that will benefit public safety operationally have yet to be realized. Thus, the manner in which public safety's ability to identify technologies and best utilize these new capabilities is yet undefined. There are, however, many applications that appear that they could use the discovery process to benefit public safety. The process of discovery could allow public safety devices to discover other users and other devices, sensors, etc. that can provide public safety users the functionality necessary to meet their operational needs. In addition, commercial development and use of discovery technologies might also allow for the establishment or enhancement of public safety operations moving forward.

The standards process of 3GPP that is working on public safety standards for Mission Critical Voice and PTT services is fluid. Throughout these discussions progress on these important issues in 3GPP has been brought to the public safety discussions and the important topics, such as public safety's ability to provision equipment and utilize Direct Communications and Direct Discovery capabilities in areas absent network coverage as compared to commercial devices, have included the ever-changing discussions on these topics within 3GPP. Simply put, the 3GPP standards associated with Direct Discovery, Direct Communications, how UE to Relay protocols operate in and out of coverage, etc., continue to change and will need to be monitored to ensure they meet public safety's needs moving forward.

The group looked forward with regard to public safety discovery and its anticipated impact to public safety users along with benefits and elements of public safety operations (applications, services, etc.) that can be enhanced by the introduction of discovery. Some of the questions and topics of discussion regarding discovery's impact to public safety operations were:

Discovery or Proximity services as defined with the 3GPP standard consists of two main elements.

- Network Authorized **Direct Discovery**. This mode of operation always requires network assistance when facilitating discovery between two Pro Se enabled UEs. This mode of operation supports UE to UE discovery when both UEs are in network coverage commercially but supports public safety UEs when only one UE is in network coverage.
- Network Independent **Direct Discovery**. Does not require any network assistance to authorize the discovery of pre-authorized public safety UEs. Communication between UEs only utilizes information local to the UEs being connected. User devices discover each other directly and interface with each without assistance from the network. Network Independent Direct Discovery can benefit public safety with facilitating discovery between devices in areas outside of network coverage. Finally, Network

Independent Direct Communication necessitates pre-configuration of UEs and enables both one to one and one to many direct communications.

Direct Communications and Direct Discovery are not permitted for commercial UEs not served by the network. Public safety enabled UEs have both Direct Communication and Direct Discovery capabilities.

Direct discovery is the ability for an authorized device to detect the presence of another discoverable device in proximity. The variables of the operating scene will need to be examined to determine “proximity” as “in building” proximities will be different areas than “outdoor” proximities. In the process of discovering devices users will need to understand that proximities and the ability to detect discoverable devices in the operating area will vary. Some urban incidents may have all devices within a small, definitive area while other, larger events by their nature can have users migrating in and out of "proximity" all of the time. The nature and size of the event and range of the devices will determine what "proximity" means in each incident.

In addition, some users will have the ability to “see” all devices and others may only be permitted to see certain devices. These parameters will be the subject of local control discussions for agencies and their users.

Direct discovery utilizes pre-configured UEs to detect the presence of another UE. Scheduling between UEs, resource allocation, and handshaking between devices are all integral elements of direct discovery and need to be implemented in the manner that best supports public safety operations. Public safety needs to be involved in the pre-configuration of devices along with testing and exercising the functionality provided in the standard to ensure the new capabilities inherent in the discovery process are beneficial to those uses in the field that can benefit from them the most. Absent any past experience in the use of discovery in public safety communications previously, the use of these capabilities will be gradual as the user base becomes familiar with the benefit and results.

Proximity services should not be limited to just other UEs but to other devices such as cameras, sensors, etc. UEs should be configured, consistent with the degree of local control as established by the agency, to discover the necessary resources in place for the event at hand and those resources could include devices that were put in place by the responding agency to support its responders in the building or in support of specific activities or functions. Further, when a device is detected, the location of the device should be known. For example, when a firefighter detects a device in a smoky building and sees that device is marking an exit to the building, the firefighter should know whether he is 5 feet or 50 feet from that sensor and exit. Knowing the location of the detected device and the distance between the user and the device is just as important as the user detecting the device in the first place.

The number of devices that are discoverable to an end user device could be many. Some coordination to the device might allow for the user to "see" more of the devices that are beneficial to him at that specific incident by reducing, at initial view, the detected devices to a minimal list of items. The user can then ask to see more of the items detected in a list until he finds the devices he needs. Utilizing profiles of users to determine the likely devices that a user might need would allow for the type of devices the user might need to be visible upon their initial inquiry. If the device is not there the user should be able to ask for more detected devices to view and possibly interface with.

Summary

This task group provided both NPSTC and PSCR valuable insight to the public safety communications listed above and confirmed the need for public safety to understand the new technologies and capabilities offered by the NPSBN as they become available. It is understood that the integration of these feature sets will be specific to the agency in a timeline that best promotes the agency's continuity of operations and support for its mission. The introduction of these new technologies necessitates agencies dedicated time and personnel to determine how the new capabilities can be integrated into the agency's operation and how those capabilities can best serve the end user.

APPENDIX D: 3GPP International Standards Information

The following information is provided to highlight how 3GPP [Third Generation Partnership] operates and to explain their work flow and process. 3GPP was created in December of 1998 as the "Partnership Project Description." The first release was "Release 1999" followed by Release 4 and subsequent sequential release identifiers.

3GPP is composed of several groups, including Organizational Partners, Market Representation Partners, and Observers. The Organizational Partners represent the top tier of the 3GPP leadership.

Organizational Partners

- ATIS (U.S.: The Alliance for Telecommunications Industry Solutions)
    - PSCR and FirstNet delegates attend via ATIS.
- ARIB (Japan: The Association of Radio Industries and Businesses)
- CCSA (China: China Communications Standards Association)
- ETSI (Europe: The European Telecommunications Standards Institute)
- TSDSI (India: Telecommunications Standards Development Society)
- TTA (Korea: Telecommunications Technology Association)
- TTC (Japan: Telecommunications Technology Committee)

Market Representation Partners include other organizations which represent stakeholders in the various 3GPP processes. They include a number of Standards Development Organizations (SDOs) and associated trade groups.

Market Representation Partners

- GSA
- GSM 95Association
- IPV6 Forum
- TD Industry Alliance
- Small Cell Forum
- Mobility Development Group (formerly CDMA)
- Cellular Operators Association of India (COAI)
- NGMN Alliance
- TCCA (Tetra Critical Communications Association)
- GCF

[95] GSMA creates Implementation Guidance documents called Permanent Reference Documents.

- CTIA
- Wireless Broadband Alliance
- 5G Infrastructure Association
- PSCE: Public Safety Communications Europe

The final category of participants are Observers, which are authorized to participate in the 3GPP proceedings, but which do not have a voting capability.

Observers

- U.S.: Telecommunications Industry Association (TIA[96])
- Canada: ICT Standards Advisory Council of Canada (ISACC)
- Australia: Communications Alliance - former Australian Communications Industry Forum (ACIF)

Work within 3GPP is organized into different Technical Specification Groups, called TSGs. These groups manage the activity within their respective areas, including the review and approval of work plans and schedules. There are three TSGs with a number of associated work groups:

1. **Radio Access Network (RAN)**
   a) RAN1 Radio Layer 1
   b) RAN2 Radio Layer 2 & 3
   c) RAN 3 RAN-CN Interface
   d) RAN4 Radio Performance
   e) RAN5 Terminal Testing
   f) RAN6 Legacy Radio

2. **System and Services Aspects (SA)**
   a) SA1 Service Aspects
   b) SA2 Architecture
   c) SA3 Security Aspects
   d) SA4 Codec Aspects
   e) SA5 OAM and Charging
   f) SA6 Critical Communications

3. **Core Network and Terminals (CT)**
   a. CT1 Terminal Aspects
   b. CT3 External Interwork
   c. CT4 Internal Protocols
   d. CT6 Smart Card applications

[96] TIA 102 covers P25 ISSI Standards, via work in the TIA TR8.8 Committee

Work in 3GPP is based on a 3GPP defined release schedule. New features are functionally frozen and are ready for implementation when a release cycle is completed. 3GPP works on a number of releases in parallel to each other, in order to maintain the continuity and momentum. For example, in 2017, Release 14 was being finalized, while work was starting on Release 15 and a project plan and scope for Release 16 was being finalized.

Work in 3GPP is further divided into, and managed, in stages.

Stage 1: The overall service description from the user's standpoint. (**Requirements**)

Stage 2: an overall description of the network functions to map service requirements to network capabilities (**Architecture**)

Stage 3: The definition of the switching and signaling capabilities needed to support services defined in Stage 1. (Adding in security, network, interface definition, test procedures) (**Protocol**, **Details**)

Work efforts at each stage are approved in a plenary meeting which includes representatives of all groups. 3GPP designated a special working group to examine public safety and mission critical services. This group is called SA-6 and the following officers were elected to leadership positions:

- Chairman, Yannick Lair, LG Electronics
- Vice Chairman, Suresh Chitturi, Samsung Electronics
- Vice Chairman, David Chater-Lee, Motorola Solutions
- Secretary, Bernt Mattsson, 3GPP Support Office

Projects and initiatives in 3GPP usually start as a Study Item in which the issue to be examined is fully discussed and preliminary conclusions are reached regarding needed capabilities and features.

Study items usually transition into Work Items. A 3GPP study contains the thinking but does not include the final conclusions. A Study Item typically concludes with the publication of a Technical Report, or "TR."

A Work Item is the next step in the 3GPP process. Work Items create Technical Specifications (called "TS") which finalize decisions discussed in the Study Phase. This is the normative phase of the work. **Normative content** defines the details which have to be complied with, or are recommended to comply with, or are possible to comply with. **Informative content** gives information or guidance to implementers, but with which it is not necessary (or possible) for equipment to ***comply*** with. Contributors in the working group process provide content to fill in the TS document. There is an established process for the receipt of contributions and how consensus is achieved in the working group.

3GPP then progresses to normative work when the studies are complete. Work flows between the various groups within 3GPP which may be impacted by the study. For example, work developed in SA6 (public safety) may flow to SA2 (system architecture) and to CT (Core Terminal and Networks). Each group has designated liaisons with other groups and questions are posted to inter-work group board.

Some of 3GPP's most important work for public safety has resolved around the creation of requirements for Mission Critical Push to Talk (MCPTT). MCPTT work has evolved over several 3GPP release cycles, with each new cycle improving on the work of the prior release. The following information provides an overview of the standards work in each 3GPP release that directly impacts public safety.

- **Release 11:** High Powered UE for Band 14/Region 2
- **Release 12:** Proximity Services
  - Device to Device Communications
  - Direct Discovery
- **Release 12:** Group Communications System Enablers
  - Support for use by Multicast/Broadcast/Unicast for application servers
  - Did not define any application layers, including MC-PTT
- **Release 13**
  - Mission Critical PTT
    - 1st mission critical application defined
    - Common services core envisioned, (more than just PTT)
  - Isolated E-UTRAN for public safety (isolated operations and secure configuration)
  - Enhancements to Proximity Services (added UE to Network relay)
  - Enhancements to Discovery and Direct Communications
  - Support for Single Cell, Point to Multi-Point transmission
- **Release 14**
  - Stage 1/Stage 2, MC-PTT split into Mission Critical general aspects (core) and MC-PTT specific aspects
  - **Common Functional Architecture (CFA)**
    - 3GPP Documents: 22.280 Stage 1/Requirements; 23.280 is Stage 2/Architecture
    - MCx common procedures (MCdata, MCvideo, MCptt)
    - Group management and configuration management
    - Added Location Management as a common function
    - Generic specification of Identities, Session, Affiliation
    - MBMS improved signaling (suspension notification), bearer aspects (announcement, quality detection, multi-server coordination) and Service Continuity.
    - **MCPTT specific enhancements**

- 3GPP Documents: 22.179 and 23.379
- Ambient Listening
- Location of current talker
- Temporary Call Group – User Regroup
- MC-PTT Private Call, Call-Back Request
- First to Answer Call Set up
- Floor Control for Audio Cut-In enabled group
- MC-PTT Emergency Alert Area (geographic area)
- MC-PTT Group Selection
- Enhanced MC-PTT Group Call Set up procedure with MBMS Bearer

▪ **Added Mission Critical Data**
- 3GPP Documents: 22.281 and 23.281
- Short Data Service (SDS)
- File Distribution
- Data Streaming
- Enhanced Status (updates of [arbitrary] status, potentially continuously **
- Transmission Control (for specific services; request indications, control timing, request transmission)
- Conversation Management (aggregate MCData transmission or a given activity
- Communications Release (termination of reception)
- Items (**) are supported Off Network as well

▪ **Added Mission Critical Video**
- 3GPP Documents: 22.282 and 23.282
- Allows video streaming from cameras or files
- Allows similar functionality to MC-PTT
  - Group Call
  - Private Call
  - Video Push**
  - Video Pull
  - Capability information sharing**
  - Transmission Control
  - Ambient Viewing
  - Support for multiple devices by a single viewer**
  - NOTE (**) are supported Off Network as well
- MCVideo has no floor control
  - Will use PTT Floor Control (chat model)
  - Requires transmission and reception control to manage network usage and user experience for group and private communications

- **Release 15**[97]
  - **Study on LMR-LTE Interworking**
    - Stage 1 requirements exist for interworking between 3GPP mission critical systems and non 3GPP mission critical systems
      - Occurred in Release 13, (see 22.179)
      - Included the eight basic NPSTC MCV requirements
    - Stage 2 work on LMR-LTE interworking is incomplete
      - Study item in progress (TR 23.782)
      - Expected to be completed in 2017
    - Scenarios have been created to identify interworking for individual features of MC-PTT and LMR/PMR
    - Private Calls
  - **Group Calls**
  - Group Management
      - Still identifying Key Issues, which will lead to the study of solutions. This will include MCData and MCvideo.
      - Normative Work awaits study completion
  - **Study on Migration and Interconnection**
    - Interconnection: allows communications between users in distinct 3GPP mission critical systems (e.g. two separate LTE networks)
    - Migration: allows a user from one 3GPP mission critical system to obtain service directly from another 3GPP mission critical system.
    - Stage 1 requirements were added in Release 13
    - Stage 2 study is in progress
      - Completion to occur by June 2017
      - Normative work awaits study completion
    - Study on **Marine Communications**
    - Study on **Future Mobile Railway Communication System**
    - Should include additional public safety enhancements work

[97] The current version of 3GPP Release 15, Section 23.379, is located here; http://www.3gpp.org/ftp//Specs/archive/23_series/23.379/

APPENDIX E: Working Group Participant List

NPSTC wishes to thank the over 250 registered members of the LMR-LTE Integration and Interoperability Working Group representing public safety, commercial, academia, and industry for their participation in the group.

NPSTC acknowledges the assistance of the following members of the Public Safety Review Team who helped conduct the final editing and review of the document:

Michael Britt, Vice Chair, Technology and Broadband Committee
Barry Fraser, Chair, Public Safety Internet of Things Working Group; BayRICS Authority
John Lenihan, Chair, Interoperability Committee; Los Angeles County Fire Department, retired
Dan Robinson, Chair, Radio Programming Compatibility Requirements; Michigan State Police
Don Root, Chair, Spectrum Committee; San Diego County Sheriff

NPSTC gives special thanks to the Working Group members who shared in the writing of this report either through participation in meeting discussions during the report writing process or as contributors to the writing and review process. The appearance of anyone's name on this list is meant to acknowledge their involvement in the process and does not automatically indicate their support, or absence of support, for the entire contents of this report.

Contributors

Dominick Arcuri, DVA Consulting
Natalie Baker, West Corporation
Mike Barney, Motorola Solutions
Jeb Benson, PSCR
Joe Boucher, Mutual Link
Kimberly Coleman Madsen, Governor's Office, State of Colorado
Norm Cook, P. Eng., Independent Consulting Engineer, Nova Scotia, Canada
Andy Davis, TIA
Stephen Devine, AT&T FirstNet
Mike Dixon, RedMobile Consulting
Tewfik Doumi, Bell Labs Consulting - NOKIA
Brice Hall, DHS/OEC
Regina Harrison, NTIA
William Janky, FirstNet
Chris Kindelspire, Grundy County ETSB 911, Illinois
Josh Lober, ESChat
Gary Monetti, Monetti and Associates
Peter Monnes, Harris Corporation

John W. Moyers, State of Tennessee, Office of EMS
Michael Newburn, County of Fairfax, Virginia
David Nolan, DHS/OEC
Tobech Ogbonna, State of Michigan, DTMB-MPSCS
Randy Richmond, Zetron
Hamlet Sarokhanian, AT&T
Dean Skidmore, IoT and LTE Consulting Group
Helen Troyanovich, State of Iowa, Iowa Communications Network
Stephen Verbil, State of Conn, DESPP/DSET
Carlton Wells, State of Florida
Peter Zwagerman, NYSTEC

Participants
Erik Anderson, Royal Canadian Mounted Police
Frederick Austin, Austin Wireless
Bruce Cox, NextNav
Peter Drozt, Motorola Solutions
David Eierman, Motorola Solutions
Chris Fish, RedCom Labs
Frank Korinek, Motorola Solutions
Xiaoyang Lee, DHS/OEC
Allen Lovett, Williamson County, TN ECD
Anthony Martwick, Sonim Technologies
Christian Militeau, West Corporation
Brett Moser, ESChat
Michael Murphy, Neptune Mobile
Harish Negalaguli, Kodiak Networks
John O'Connor, City of Memphis FD, Tennessee
Rodney A. Olson, City of Minneapolis, Minnesota
Mark Raczynski, General Dynamics Mission Systems
Betty Rinehart, Rinehart Spectrum Solutions Group, LLC
Mel Samples, CADSTAR, Inc.
Charlie Sasser, NASTD
Michael Sasuta, MDS Concepts Unlimited
DeWayne Sennett, AT&T
James Stefano, RIT
Jeff Stock, Buford, Goff and Associates Inc.
Tim Thompson, Electronics Engineer - NIST | CTL | PSCR