A NPSTC Public Safety Communications Report

The National Public Safety Telecommunications Council is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Public Safety Broadband High-Level Launch Requirements

Statement of Requirements for FirstNet Consideration

December 7, 2012

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC), and the National Protection and Programs Directorate, Office of Emergency Communications (OEC), for their support.

American Association of State Highway and Transportation Officials | American Radio Relay League | Association of Fish and Wildlife Agencies | Association of Public Safety Communications Officials | Forestry Conservation Communications Association | International Association of Chiefs of Police | International Association of Emergency Managers | International Association of Fire Chiefs | International Municipal Signal Association | National Association of State Chief Information Officers | National Association of State Emergency Medical Services Officials | National Association of State Foresters | National Association of State Technology Directors | National Emergency Number Association | National Sheriffs' Association

191 Southpark Lane, #205 | Littleton, CO 80120 | Phone 866-807-4755 | Fax 303-649-1844 | Website www.NPSTC.org

Intentionally Blank

Document Notices

Following is publication information for this document.

Abstract

This document contains high-level launch requirements for an interoperable public safety broadband communications nationwide network to serve all local, tribal, state, and federal first responder communications.

The National Public Safety Telecommunications Council (NPSTC) is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

Acknowledgements

This document was drafted by NPSTC's Broadband Working Group (BBWG) and approved in final form by the NPSTC Governing Board on December 7, 2012.

Contact Information

Support Office

8191 Southpark Lane, Unit 205

Littleton, CO 80120-4641

Fax: (303) 649-1844

Toll Free: (866) 807-4755

NPSTC: support@npstc.org

NIIX: support@niix.org

NPSTC Administration

Marilyn Ward, Executive Director

mward@npstc.org

http://www.npstc.org/

For more information, see http://www.npstc.org/ContactUs.jsp.

Intentionally Blank

Executive Summary

The recent passage of the Middle Class Tax Relief and Job Creation Act of 2012 [1] has enabled the reality of the deployment of the Nationwide Public Safety Broadband Network (NPSBN). This groundbreaking legislation establishes the governance and identifies the funding necessary to transform the way public safety practitioners communicate. One could equate the current position to the early days of land mobile radio when its deployment reduced the reliance on telegraph and call box systems. That major transformation in communications modality transformed the delivery of public safety services more than 50 years ago. Public safety is, again, on the verge of a similar transformation in the way responders communicate.

The First Responder Network Authority's (FirstNet) deployment and operation of the NPSBN depends on the articulation of public safety's technical and administrative requirements in the immediate, medium, and long-terms. The National Public Safety Telecommunications Council (NPSTC) prepared this document to articulate immediate-term, must-have launch requirements as part of its ongoing efforts to help improve public safety communications.

This high-level launch statement of requirements has been developed by public safety practitioners from all disciplines, experts in public safety communications, commercial wireless providers, members of the academic community, information technologists, equipment manufacturers, and many others who have dedicated numerous hours because they know they are contributing to one of the most important technology initiatives of their careers.

Purpose of this Document

The principal purpose of this document is to define, from the perspective of NPSTC, high-level broadband public safety launch requirements for consideration by the FirstNet. The high-level launch requirements have been developed principally based on:

- NPSTC review of the governing legislation, Public Law 112-96, Middle Class Tax Relief and Job Creation Act, specifically Title VI of that Act, Public Safety Communications and Electromagnetic Spectrum Auctions, Section 6001 et seq. Throughout this document, Public Law 112-96 shall be referred to as "the legislation."
- Review of prior efforts conducted by NPSTC to define public safety's requirements for broadband networks, services, applications, and other capabilities.

Extensive inputs and comments by a wide variety of stakeholders in public safety communications, including representatives of the U.S. first responder community, local, tribal, state, and federal organizations and agencies, and domestic and international communications service providers, manufacturers, and other industry segments, and consultants. A secondary purpose of this document is to establish a baseline for an iterative process to develop successively more detailed public safety requirements as the NPSBN evolves based on FirstNet's decisions in deploying, administering, operating, maintaining, and evolving the NPSBN.

The document defines certain requirements to support local operations which are critical for the flexibility required by local, tribal, state, and federal to successfully utilize the network to protect their constituent populations.

It also includes the identification of key challenges and considerations, both technically and administratively, to successfully implement the NPSBN consistent with the legislation. Such challenges and considerations include: funding, time-to-market, urban/rural coverage, data rates/quality of service, access to user equipment, mission-critical voice over long-term evolution (LTE), application development/management, local versus national control of the NPSBN, roaming to commercial service providers, continuity of operations/resiliency/reliability/security, and cyber security and other threats to the network and devices.

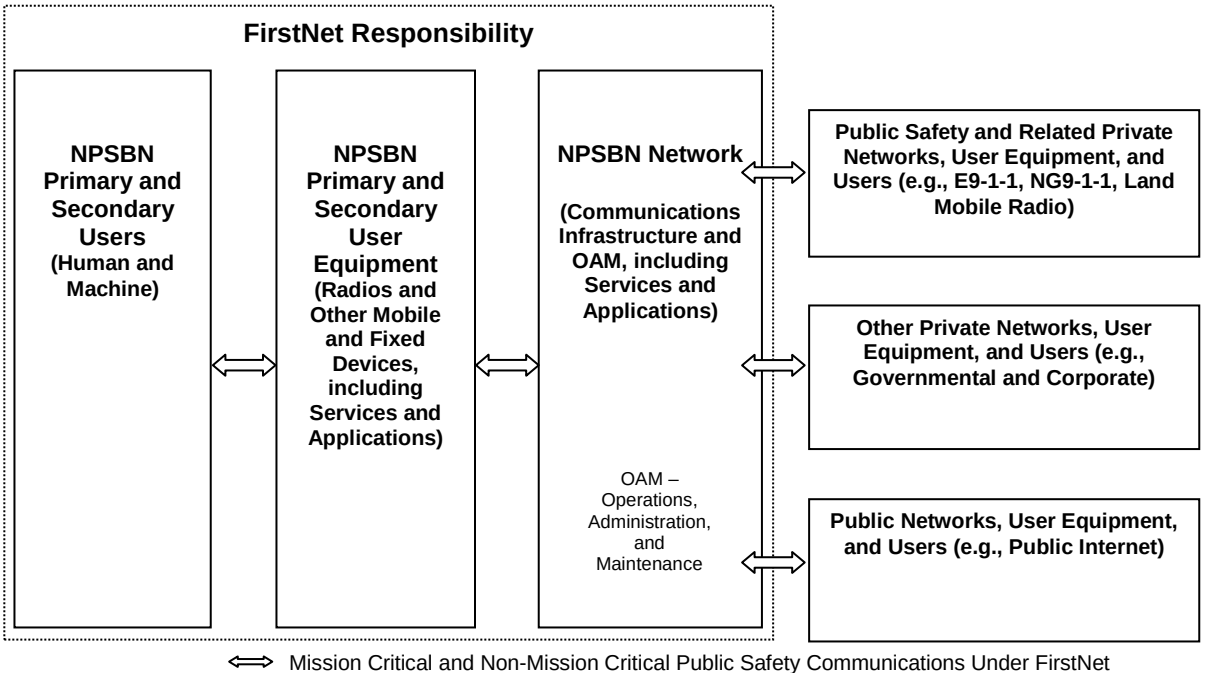
This document identifies launch requirements for FirstNet and the NPSBN that are derived from the needs of the majority of potential adopters of the system. As a result, this document:

- Excludes any direct discussion of the Opt-Out alternative.
- Excludes any direct consideration of any early builder[1] currently granted or pending, although NPSTC recognizes the benefits early builders can bring to FirstNet.
- Excludes any discussion or repetition of the FCC Interoperability Board minimum interoperability requirements, as they are already specified and readily available to FirstNet.
- Excludes any discussion of implementation solutions as the intent of the document is to present the *What* and not the *How*.
- Excludes design of the NPSBN, as that is the responsibility of FirstNet.
- Excludes any discussion of international alternatives when discussing possible Public-Private Partnerships, although such alternatives are not discouraged.
- Excludes the development of quantitative administrative and technical requirements for achieving interoperability between NPSBN and non-NPSBN users.

The scope of the high-level technical and administrative requirements defined in this document focus principally on defining NPSBN capabilities under FirstNet responsibility, which is illustrated in the figure below.

[1] "Early builders" are members of the Early Builders Advisory Council (formerly known as "the waiver recipients) who comprised the Public Safety Spectrum Trust Operator's Advisory Committee.

Figure 1. NPSBN Capabilities under FirstNet Responsibility



Goal of FirstNet

FirstNet will be responsible for building and maintaining the NPSBN, either directly or indirectly through a partnership. The NPSBN includes the Radio Access Network (RAN), backbone and core, which encompass the control logic, user information repositories, and nationwide fiber network. States will be involved in the requirements definition of the network, but specifically will be responsible for coordinating the RAN portion of the NPSBN in their respective states. Each state is responsible for working with FirstNet to negotiate the coverage and capacity considerations for their state.

Coverage and Capacity

Public safety has been using data in some form or fashion for a number of years. As with the general public, multi-media data usage is beginning to explode in public safety. Unlike the general public, a public safety data network requires virtually ubiquitous coverage driven by user needs versus revenue potential. Not only is coverage critical, also of great importance is capacity. Most large-scale public safety events are somewhat localized leading to large concentrations of users (i.e., several hundred users in less than one square mile). This coverage and capacity are needed in times that task traditional networks such as major events, large-scale disasters, and during extended periods without available commercial power. Commercial networks are not generally designed for these extreme demands on coverage or capacity requirements.

Priority

During an emergency, not all public safety users are created equal. Some users, applications, and situations require elevated access levels depending on various factors and authorizations. Therefore,

public safety requires a very robust prioritization scheme that can be enacted at the local level. This is especially true in large-scale events that have established hierarchy with role-based levels of priority. Some situations are of such critical importance that certain network traffic should be able to pre-empt lower level traffic. Strict controls and national standards need to exist for this type of pre-emption to curtail any potential abuse.

Resiliency

Public safety responders need to be able to exchange information even when any piece of the network is unavailable due to failure, such as in the event of a natural disaster. This makes off-network, peer-to-peer, and self-healing capabilities critically important. Redundancy is one traditional approach to building high availability networks, but high network availability could be achieved by designing the network with resiliency, which could result in a lower deployment cost.

Security

Public safety processes sensitive information on a daily basis, which requires robust security measures to ensure integrity, confidentially, privacy protection, and information assurance. A nationwide public safety broadband network would be an obvious target for cyber attack. This fact requires that extensive security measures be enacted to prevent attacks on the network to include but not be limited to cyber-attacks, physical site security, and denial of service.

NPSBN High-Level Requirements

The establishment of high-level technical and administrative launch requirements for the NPSBN will form a firm foundation for subsequent detailed requirements for the NPSBN and expected support activities that FirstNet will undertake.

The high-level launch requirements defined in this document are intended for FirstNet consideration in its design, development, deployment, operation, and evolution of the NPSBN.

Managing Expectations

Although this Statement of Requirements document describes the “Launch Day” needs of public safety, there are features and functionality not listed that require the attention of FirstNet. Any Request for Proposal (RFP) issued by FirstNet should be written to leverage the efficiency of a long-term vision during the initial build out. For example, if mission critical voice is envisioned to become part of the NPSBN, the RFP should consider this in defining coverage requirements.

Various requirements in this document refer to public safety grade (PSG). While the meaning of this terminology was not defined at the time of this document’s completion, the NPSTC Broadband Working Group (BBWG) plans to define the terminology as quickly as possible, for use by FirstNet in system design. For now, the intent of the PSG terminology is to convey the need for design choices that support a greater overall network reliability and resiliency to network disruptions compared to commercial

networks. PSG terminology must be completed prior to any deployment of equipment or finalization of design documents and specifications.

While this document provides recommendations for the implementation of a dedicated public safety network, a number of real-world issues will challenge the design and implementation of the NPSBN. Members of the public safety community, FirstNet, and other interested parties should, from the outset, be prepared to manage their expectations related to this unprecedented undertaking. Implementation of the NPSBN will not happen overnight. Network implementation may well mirror network deployments by commercial operators. It is important to understand that no commercial network operator has ever turned on a nationwide network all at one time.

Potential users of the NPSBN must recognize that some users will have access to the network earlier than others. Equally, there is currently no user equipment ecosystem for band class 14 devices, the spectrum allocated to the NPSBN. Users who are accustomed to a wide variety of handsets, tablets, and portable Wi-Fi devices, will have to wait for the time that these types of devices become available. Also, current discussions regarding mission critical voice over LTE networks will have to be addressed. Additionally, the definition of PSG for all services needs to be agreed upon prior to implementation. These and a host of other issues deserve focused attention by FirstNet, the public safety community, and the policy makers who will be watching the development of the NPSBN with considerable attention.

Intentionally Blank

Contents

Tables

Figures

1 Introduction

This section introduces basic concepts to understand about the document while reading the high-level launch requirement sit identifies. Appendix A provides a list of acronyms and abbreviations used in the document.

1.1 Purpose of this Document

The principal purpose of this document is to define, from the perspective of the National Public Safety Telecommunications Council (NPSTC), high-level broadband public safety launch requirements for consideration by FirstNet as it embarks on its mission to deploy the nation's first nationwide public safety broadband network.

1.2 Scope of this Document

The scope of this document is limited to the preliminary definition of high-level launch requirements for FirstNet's consideration in the deployment of the Nationwide Public Safety Broadband Network (NPSBN).

1.2.1 Long-Term Vision for NPSBN Build Out

Following are important features and functionality deferred from the "Launch Day" requirements. Most or all of these features will return for the later stages of build out. The initial design of the network should consider the impact of adding these features later in the build out and strive to avoid any costly retrofits down the road.

- Direct-mode mission-critical push-to-talk (PTT) voice
- User Equipment
- Off network (Direct) communication – both voice and data
- Peer-to-peer
- Point to multi-point
- NPSBN-Hosted applications
- Identity management credential hosting
- Accounting

- Administrative interface
- Problem ticket
- General activity and usage
- Billing data reporting for current period on an ad hoc basis
- User-defined fields for activity reporting
- Data sharing policies

1.2.2 Public Safety Grade to be Defined

Various requirements in this document refer to public safety grade (PSG). While the meaning of this terminology was not defined at the time of this document's completion, the NPSTC Broadband Working Group (BBWG) plans to define the terminology as quickly as possible, for use by FirstNet in system design. For now, the intent of the PSG terminology is to convey the need for design choices that support a greater overall network reliability and resiliency to network disruptions compared to commercial networks. The goal is for the NPSBN to be equivalent to public safety land mobile radio (LMR) systems that support law, fire, and emergency medical service (EMS) operations and are commonly referred to as "mission-critical systems."

Reliability is achieved in public safety LMR systems through equipment redundancy and minimizing single points of failures. System operators stock spare parts and, in some cases, transportable backup systems to restore system failures that do occur. Reliability is achieved through careful system design and must be considered at the earliest stages of system design.

Resiliency is achieved through careful considerations of local environmental factors and how events such as earthquakes, wildland fires, hurricanes, floods, lightning, ice, tornadoes, and even vermin can disrupt or damage the NPSBN network. Consideration to common atmospheric conditions such as extreme temperature shifts, high/low humidity, or even salty air affects resiliency. One failure common to all types of natural disasters is the commercial power service. Public safety LMR systems incorporate both battery and backup generators at the radio sites to insure reliable power for the equipment. The size and type of batteries and generators vary from region-to-region depending on a number of factors. Each disaster type requires different consideration for what is required to ensure network resiliency. Resiliency is designed into the network starting at the earliest stages of system design.

1.3 Nomenclature for Preliminary High-Level Launch Requirements

Requirements in this document are enumerated in tables and informative text is provided outside of the tables. The next table provides an example. A description of each column follows.

#	Requirement
1	
2	

3	

The requirements tables include the following columns:

- **# – Requirement Number** – A unique identifier for the requirement.
- **Requirement** – Text describing the requirement being satisfied by the initial deployment (launch) of the NPSBN.

1.4 Definition of an NPSBN User

The safety of the public *and* that of the nation's first responders demands that the primary user base of the NPSBN should include those entities and services that are essential to ensure timely and effective response to emergency events whether local, tribal, state, federal, or international in scope.

Accordingly, the *Middle Class Tax Relief and Job Creation Act of 2012* [1] defines NPSBN users in Title VI, *Public Safety Communications and Electromagnetic Spectrum Auctions*(Spectrum Act). The Act states that users include entities that provide *public safety services*, where *public safety services* encompasses the definition of *public safety services* outlined in the *Communications Act of 1934* [2] and the definition of *emergency response providers* in the *Homeland Security Act of 2002* [3].

- Section 337(f) of the Communications Act defines *public safety services* as the sole or principal purpose of which is to "protect the safety of life, health, or property; that are provided by state or local government entities; or by nongovernmental organizations that are authorized by a governmental entity whose primary mission is the provision of such services; and that are not made commercially available to the public by the provider."
- Section 2 of the Homeland Security Act of 2002 defines *emergency response providers* as including "Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical(including hospital emergency facilities), and related personnel, agencies, and authorities."

Additionally, and for purposes of efficiency in investment and in use, the Spectrum Act also allows for non-public safety users of network capacity and equipment/infrastructure on a secondary basis. Such secondary users will be governed by covered lease agreements that are written agreements for public-private partnerships to construct, manage, and operate the NPSBN between FirstNet and the secondary users.

Taken together, the NPSBN user base should include any emergency response agency or authority with Emergency Support Function (ESF) responsibilities, including but not limited to, traditional and non-traditional first responder entities, as defined in the National Response Framework (NRF) as lead and supporting agencies (e.g., utilities, public works, hospitals, transit, transportation, military, National Guard, and others). Although all of these users may not be traditional first responders, they are often critical support in the mitigation of incidents. The First Responder Network Authority (FirstNet) should determine a common methodology to determine when these users become part of the incident

response and their role on the network during routine non-emergency conditions. Following are requirements for defining an NPSBN user (NPSBN-U).

Table 1. Definition of NPSBN User Requirements

#	Requirement
1	FirstNet SHALL define the requirements for agencies and/or authorities to qualify as NPSBN users.
2	FirstNet SHOULD include any emergency response agency and/or authority with ESF responsibility as outlined in the NRF.

1.5 Document Organization

This document is organized as follows.

The Executive Summary highlights the key information contained in the document, including the document's principal conclusions and recommendations.

Section 1 provides an overview, including identification of the scope and purpose of the document.

Section 2 defines high-level NPSBN governance requirements for FirstNet Board consideration.

Section 3 defines high-level policies and NPSBN procedures requirements for FirstNet Board consideration.

Section 4 defines must-have for launch technical requirements for FirstNet Board consideration.

Section 5 defines security requirements.

Section 6 defines priority and quality of service requirements.

Section 7 summarizes the conclusions and recommendations for this document.

Section 8 identifies the references cited in this document.

Appendix A provides a list of acronyms and abbreviations used in this document.

2 Governance

There are more than 50,000 public safety agencies across the nation. The laws and policies of each respective jurisdiction or defined area of responsibility for each jurisdiction govern each agency. Until now, no single entity has existed with authority to support and manage a nationwide emergency communications network for users across local, tribal, state, and federal governments and agencies. With the establishment of the NPSBN, formal governance structures extending from FirstNet to all users are needed to manage this new system of applications, user equipment (UE), users, and network infrastructure.

2.1 Local/Tribal/State/Federal Governance

To effectively coordinate statewide governance and receive insights from all stakeholders, existing statewide communication governance models should be leveraged to incorporate the input of the entire local, tribal, state, and federal stakeholder communities. For this to happen successfully, the structure cannot be top-down or exclusive but instead should be collaborative and inclusive of all stakeholders.

Some Statewide Interoperability Governing Boards (SIGB) and Statewide Interoperable Executive Committees (SIEC) have formed specific public safety broadband committees. Some states also have state broadband task forces addressing commercial and public safety broadband needs and requirements. FirstNet should leverage technical and operational support as it exists within the states and consider what existing local, tribal, state and federal governance can offer to the deployment of the NPSBN. Following are collaboration requirements for local, tribal, state and federal governance.

Table 2. Local/Tribal/State/Federal Governance Requirements

#	Requirement
1	FirstNet SHOULD collaboratively leverage existing statewide communication governance models to incorporate the input of the entire local, tribal, state, and federal community.
2	FirstNet SHOULD leverage technical and operational support as it exists within the states and consider what existing local, tribal, state and federal governance can offer to the deployment of the NPSBN.

2.2 Tribal Governance

The Spectrum Act requires FirstNet to consult with “tribal entities” in the building, deployment, and operation of the NPSBN. It also requires FirstNet to consult with “tribal jurisdictions” in carrying out requests for proposals (RFP) and other responsibilities regarding the distribution and expenditure of funds. However, the Act does not define “tribal entities” or “tribal jurisdictions,” leaving FirstNet to determine which tribal groups to include and to what extent they will be involved in the consultation process.

The 566 federally recognized American Indian tribes have a government-to-government relationship with the United States with certain established responsibilities, powers, limitations, and obligations. As FirstNet consults with these federally recognized tribes, FirstNet should acknowledge and consider existing issues of tribal sovereignty and federal trust principles in the development of the NPSBN.

FirstNet should work with the U.S. Department of Interior's Bureau of Indian Affairs (BIA), the Federal Communications Commission's (FCC) Native American Bureau, and other groups with strong working relationships among tribal groups to help determine wherein lie gaps specific to the needs of public safety among both urban and rural tribal groups. An understanding of these issues will facilitate positive working relationships between the new governance entity, FirstNet, and the various tribal entities. Following are requirements for tribal control.

Table 3. Tribal Control Requirements

#	Requirement
1	FirstNet SHALL consult with tribal entities in the building, deployment, and operation of the NPSBN.
2	FirstNet SHALL acknowledge and consider existing issues of tribal sovereignty and federal trust principles in the development of the NPSBN.

2.3 Federal Agency Governance

Title XVIII of the Homeland Security Act as amended in 2007 established the Emergency Communications Preparedness Center (ECPC).The Secretary of Homeland Security, the Chairman of the Federal Communications Commission, the Secretary of Defense, the Secretary of Commerce, the Attorney General of the United States, and the heads of other federal departments and agencies or their designees jointly operate the Center.

The ECPC improves emergency communications collaboration across the federal government and aligns initiatives with national-level policy and guidance. The ECPC is designed to increase efficiencies at the federal level, improve alignment of strategic and operational emergency communications planning and across levels of government and leverage the collective member resources to drive research and development and standards for existing and emerging technologies.

Table 4. Federal Governance Requirements

#	Requirement
1	FirstNet SHALL leverage the ECPC to effectively coordinate with federal agencies and to develop partnerships with federal agencies to support the deployment, security, and operation of the NPSBN.

#	Requirement
2	FirstNet SHALL leverage technical and operational support as it exists within the federal user community and consider what existing federal governance can offer to the deployment of the NPSBN.

2.4 Public and Private Governance

FirstNet should consider who drafts lease and partnership agreements, how such relationships will function, the process for oversight, and the process for identifying partners. Partnerships will benefit FirstNet as well as NPSBN stakeholder agencies and end users. FirstNet should consider developing partnerships from the perspectives of local, tribal, state and federal entities as well as any relationships with industry partners.

FirstNet should also consider what such partnerships will cover beyond equipment/infrastructure sharing. FirstNet may need to overcome legal/regulatory barriers, such as grants and appropriations-related issues, limits of liability, credentialing, and identification of commercial entities providing/supporting critical public safety services. Federal and state laws should be examined for potential conflicts with an eye toward resolving such matters before agreements are issued and should develop templates, processes, and approaches to streamline regulatory/permitting issues. Following are requirements for public and private governance.

Table 5. Public/Private Governance Requirements

#	Requirement
1	FirstNet SHALL consider partnerships from the perspective of nationwide, local, tribal, multi-state and federal entities and any relationships with industry partners.
2	FirstNet SHALL attempt to overcome any legal/regulatory barriers identified, such as grants and appropriations related issues, limited liability, credentialing, and identification of commercial entities providing/supporting critical public safety services.

Intentionally Blank

3 Policies and Procedures

Agencies often create policies and procedures to meet their unique emergency communications requirements. In recent years, with support from the federal government, emergency responders have developed standards for interoperability, the use of existing nationwide interoperability frequencies, and incident management. However, with FirstNet, disparate policies and procedures will need to be consolidated and made consistent to all end users. Technical requirements identified in this document can provide a basis for service level agreements (SLAs) and accountability. Technical and/or other service requirements identified by entities/users should provide a basis for accountability in service level agreements (SLAs) or other types of agreements. Additionally, other sections may contain policy and/or procedure-related requirements on topics which are not covered in Section 3.

As a matter of policy, NPSTC recommends that FirstNet offer support to states as they partner and negotiate with new and existing commercial providers for appropriate terms of service specific to public safety enterprise network (PSEN) users, where a PSEN is a communications network that serves one or more public safety agencies. A PSEN can serve an entire state or a single agency. In this document, a public safety entity (PSE) is synonymous with a public safety agency responsible for operations and maintenance (O&M). For example, procedures may be negotiated to permit NPSBN users (NPSBN-Us) needing to roam onto commercial networks so they receive consistent treatment of their assigned priority classifications, such as through admission control (AC), allocation and retention priority (ARP), and/or quality of service class identifier (QCI), commensurate with their PSE identity.

3.1 User Prioritization

The NPSBN presents an entirely new dynamic to management of communication resources. Comparisons between today's LMR systems and tomorrow's LTE systems are often misleading and inaccurate when user priority is discussed. LMR system priorities are applicable across the footprint of the system, while LTE prioritization schemes effectively limit the impact to users within a single cell sector. High-user traffic in one sector has little impact on users in other cell sectors.

Priority, QoS, and Pre-emption are essential attributes of a mission critical system. Responders must have the resources they need to complete their mission. A nationwide framework is necessary which balances the needs of all agencies sharing the NPSBN, yet the framework must not be too rigid as to ignore the dynamic nature of all incidents. FirstNet must develop a policy for the NPSBN that requires a nationwide standard for prioritization and quality of service (QoS). Prioritization is the network's ability to determine the priority level of a connection over another for access to, transport through, and egress from the network. QoS is the network's ability to ensure that Internet Protocol (IP) packet flows associated with different applications satisfies performance objectives for different applications to operate. Thus, prioritization addresses the network connection while QoS addresses the treatment of traffic after the connection is established.

Prioritization in the NPSBN must ensure that high-priority users can establish connections with a high level of certainty relative to low-priority users. Priority levels for connections may be defined and assigned based on various criteria including the user's role, user application types, or incident type. In addition, public safety applications such as Computer Aided Dispatch (CAD), Incident Command System (ICS), Next-Generation 9-1-1 (NG9-1-1), and other applications that require QoS support for their proper operation will require standardized mechanisms to inform the network of the prioritization and QoS attributes of these IP packet streams.

Although the technical aspects associated with management of priority and QoS on an LTE network are standardized, the dynamic factors associated with incident management prevent a simple consistent approach to dynamically assigning priority based on a user's role in an incident. It is typically not possible to predict which user or how often an agency must have the highest priority at any particular moment.

The NPSTC Priority and QoS Working Group identified two public safety network services that must have high priorities: responder emergency and immediate peril [4]. Further categories are defined in Section 6 including ICS Incident Priority and Itinerant User. Therefore, the NPSBN should utilize a base nationwide priority scheme for users and applications on the network. The priority scheme must reserve the highest levels of priority for the applications mentioned above (responder emergency and immediate peril). Nothing on the network should have a higher priority. Below those two levels, NPSTC recommends that FirstNet establish priorities for operational units of law enforcement, fire, EMS, and emergency management agencies. The priorities for the operational elements of these four services should be consistent across the network.

The lowest network priorities must be reserved for those users who lease the spectrum for commercial and/or personal use. Although assigned to the lowest system priorities, these users will typically not experience any performance limitations unless a major public safety event is active in the same cell sector. Following are requirements for user prioritization.

Table 6. User Prioritization Requirements

#	Requirement
1	FirstNet SHALL develop a policy for the NPSBN that requires a nationwide standard for prioritization and QoS.
2	FirstNet SHALL define the default priorities of all user classes on the NPSBN.
3	FirstNet SHALL establish a policy whereby public safety applications such as CAD, ICS, and other applications that require QoS support for their proper operation will utilize standardized mechanisms to inform the network of the prioritization and QoS attributes of these IP packet streams.

#	Requirement
4	Pursuant to Section 6211 of the Act, Responder Emergency and Immediate Peril SHALL have the high priorities on the NPSBN or on a commercial wireless network.
5	The lowest network priorities SHALL be reserved for those users who lease the spectrum for commercial and/or personal use.

3.2 PSEN Policy

PSENs represent networks owned and operated by PSEs that support localized applications and services such as application layer authentication, QoS management, security management, CAD, application services, public safety answering points (PSAP), and other operational aspects of public safety organizations. A PSEN can serve an entire state (multiple PSEs) or a single agency (i.e., a single PSE). PSENs may include administrative and management functions of the public safety organization.

Connectivity policies for PSENs should specify access requirements by authorized NPSBN-Us. In addition, the PSENs should coordinate security policy and procedures with the NPSBN security team. The initial connectivity at launch should be as simple as allowing secure VPN access. Following are policy requirements for PSEN connectivity.

Table 7. PSEN Connectivity Policy Requirements

#	Requirement
1	FirstNet SHALL establish a policy to enable PSENs and PSEN applications to be accessed via the NPSBN.
2	The NPSBN and PSEN networks SHALL have the ability to terminate and or restrict the connectivity between the networks if situations where a threat may be detected. The organizations SHALL have procedures in place for notification of action and negotiation of correction procedures.

3.3 Migration from Existing Public Safety Private Wireless Data Networks

This section describes decision making, responsibilities, and technical requirements associated with the elective migration of existing public safety private wireless network data connectivity onto NPSBN infrastructure to establish best practices and lessons learned. This section focuses on recommendations to FirstNet oversight regarding migration. Topic areas include:

- Decisions to migrate
- Planning
- Implementation

- Life-cycle management
- Security management
- Network availability management

Where requirements in this section reference consultations between FirstNet and Network Administrators, Network Administrators represent local, tribal, state, and federal authorities, as defined in Spectrum Act [1] sections 6206(c)(2) and 6302(d).

Following are requirements for migration of private data networks.

Table 8. Private Data Networks Migration Requirements

#	Requirement
1	FirstNet administration SHALL establish an advisory body to assist PSE jurisdictions in migrating existing private wireless network data connectivity onto the NPSBN.

3.4 Network Interoperability Certification

FirstNet should maintain network interoperability across the NPSBN. A certification process for network hardware and firmware should be developed, implemented, maintained, and enforced across all components of the network. Following are network certification requirements for interoperability.

Table 9. Network Interoperability Certification Requirements

#	Requirement
1	FirstNet SHALL establish a certification process for all network hardware and firmware.
2	FirstNet SHALL establish a policy to insure that all applicable components of the network comply with the Network Interoperability Certification Requirements.

3.5 Provisioning

FirstNet should develop and maintain standard operating procedures at the local, tribal, state, and federal agency level that will define the process for provisioning users. These procedures should include adding, updating, and removing UE access from the NPSBN. A template for UE provisioning should be developed and maintained by FirstNet. Following are NPSBN requirements for provisioning.

Table 10. Provisioning Requirements

#	Requirement
1	FirstNet SHALL develop and maintain standard operating procedures at the local, tribal, state, and federal agency level that will define the process for provisioning users.

3.6 Technology Evolution

This section provides requirements focused on evolution and upgrade of the network. The topic areas include roadmap and feature planning, configuration management, upgradability and backwards compatibility, life cycle management, coverage and capacity management, network availability management, and network security management.

Administrative services (security, provisioning, upgrades, etc.) provided by FirstNet shall provide the same level of features/capabilities as commercial providers do – at a minimum.

3.6.1 Roadmap and Feature Planning

Roadmaps should include multiple facets of technology evolution and planning. At a minimum, roadmaps should include:

- Radio access network (RAN) build-out
- Early builder integration
- Software upgrade
- Feature phasing
- Capacity expansion
- Technology upgrade/inflection
- Management process roll-out

Following are requirements for roadmap and feature planning.

Table 11. Roadmap and Feature Planning Requirements

#	Requirement
1	The NPSBN SHALL support future defined applications as required by PS Users and as sanctioned by FirstNet.
2	FirstNet SHALL implement a coverage and capacity expansion plan.
3	FirstNet SHALL implement process-improvement procedures for roadmap management including feature-request and feature-prioritization processes.

3.6.2 Upgradability and Backward Compatibility

The objective of upgradability requirements is to minimize impacts of software upgrades on hardware. However, some system features such as higher-order multiple-input multiple-output (MIMO) and evolved multimedia broadcast multicast services (eMBMS) will require deployment of new and/or additional hardware. Following are requirements for upgradability and backward compatibility.

Table 12. Upgradability and Backward Compatibility Requirements

#	Requirement
1	FirstNet SHALL plan and maintain budget items for upgrades and technology refresh according to the established roadmap.
2	FirstNet SHALL implement an upgrade/maintenance coordination and notification process with all appropriate partners.
3	FirstNet SHALL maintain backwards compatibility with deployed UEs as allowed by 3GPP standards.
4	Infrastructure upgrades for the NPSBN SHALL be performed in such a way as to minimize outage areas, such as upgrading sites that are not adjacent.

3.6.3 Life-Cycle Management

Following are requirements for life-cycle management.

Table 13. Life-Cycle Management Requirements

#	Requirement
1	FirstNet SHALL implement life-cycle management processes for interfaces exposed to applications, O&M Users, LTE Users, Non-LTE Users, and Network Administrators.

3.6.4 Coverage and Capacity Management

Following are requirements for coverage and capacity, and roaming.

Table 14. Coverage and Capacity and Roaming Requirements

#	Requirement
1	FirstNet SHALL implement a coverage and capacity expansion plan.
2	In conjunction with NPSBN service, a commercial cellular roaming agreement SHALL be offered.
3	The NPSBN SHALL be capable of delivering a similar suite of features, functions, and capabilities as available over commercial cellular networks.
4	Commercial carrier roaming agreements for NPSBN subscribers SHALL incorporate input from Network Administrators to ensure local, tribal, state, and federal requirements (e.g., QoS needs) are met.

#	Requirement
5	A migration plan from the commercial cellular network to the NPSBN SHALL be developed in collaboration between Network Administrators and FirstNet.
6	A commercial cellular system to NPSBN migration strategy SHALL be developed that supports co-existence on both the cellular network and NPSBN for a sufficient timeframe to manage the successful migration.
7	A commercial cellular system to NPSBN transition test plan SHALL be provided to assist migration to the NPSBN.

3.7 Maintenance Policy

Regularly scheduled network maintenance will be conducted on the NPSBN. Hardware and firmware updates on the network may make the network unavailable to users during the update process. Users should be notified of all system updates that may require the system to be unavailable. Such maintenance policies should be incorporated into all SLAs. Following are NPSBN requirements for maintenance policy.

Table 15. Maintenance Policy Requirements

#	Requirement
1	FirstNet SHALL establish a policy to schedule network maintenance.
2	FirstNet SHALL establish a policy to notify users of scheduled maintenance that may impact the user experience on the NPSBN.

3.8 Billing Support Systems

Following are requirements for billing support systems.

Table 16. Billing Support Systems Requirements

#	Requirement
1	FirstNet SHALL develop policies regarding the billing of users and/or user agencies that reconcile usage by individual agencies and jurisdictions.
2	FirstNet SHALL use the Network Numbering Schema developed by the Public Safety Spectrum Trust (PSST) Operators Advisory Council (OAC) as a foundational element of the billing system.

3.9 Network Monitoring

Network Operations Center (NOC) functionality will be needed to support the NPSBN on a 24x7x365 basis. An agreement between FirstNet and local, tribal, state, and federal entities should be developed for monitoring the network, repairs, and upgrades. These policies should leverage existing policies and information from local-, tribal-, state-, and federal-based organizations for troubleshooting, network restoration, and help desk functions. Following are NPSBN requirements for network monitoring.

Table 17. Network Monitoring

#	Requirement
1	FirstNet SHOULD develop a policy defining the ability and process for local, tribal, state, and federal entities to monitor the network.
2	FirstNet SHALL establish policies to provide user entities prompt trouble reports, information helpful to facilitate operations using contingency communications, and restoration reports.
3	FirstNet SHALL establish a policy to provide user entities insight into overall system performance metrics, including availability and coverage.

3.10 Training and Exercises

Training and exercises play a vital role in preparedness, readiness, and proficiency in accessing and using communications capabilities during emergency events. Preparedness is essential to ensuring that NPSBN equipment is well maintained and operational. Achieving appropriate levels of readiness and proficiency ensures that personnel can deploy, set up, and use the NPSBN equipment effectively, both on their own and in conjunction with other emergency responders. Following are requirements for NPSBN equipment training and exercises.

Table 18. Training and Exercise Requirements

#	Requirement
1	FirstNet SHALL establish standardized training programs to deliver to all personnel who manage NPSBN communications resources.
2	As FirstNet deployed applications become available, FirstNet SHALL conduct training for the NPSBN within agencies, across disciplines, jurisdictions, and levels of government, and with key private sector organizations as required.

3.11 Standard Procedures Across Agency Levels

FirstNet must ensure that emergency response agencies across all levels of government have adopted and implemented policies and guidance to ensure common NPSBN use and support. Implementation of

these policies will establish clearly defined roles and responsibilities and enable integration of all elements of the NPSBN.

Procedures for the activation, deployment, and deactivation of technical resources should be included, as well as roles and responsibilities for the operation, management, recovery, and continuity of NPSBN equipment and infrastructure.

FirstNet should provide flexible contracts. These contracts should be written to allow local and tribal jurisdictions and individual states the ability to procure goods and services without individual violation of procurement acts or policies.

Following are requirements for standard procedures across agency levels.

Table 19. Standard Procedures Requirements

#	Requirement
1	FirstNet SHALL implement policies and guidance to ensure common NPSBN use and support.
2	FirstNet SHALL implement procedures for the activation, deployment, and deactivation of technical resources.
3	FirstNet SHALL provide support for procurement of goods and services.
4	FirstNet SHALL provide a continuity of operations (COOP) and continuity of governance (COOG) plan that is reviewed, updated, and exercised as needed, but not less than annually.

Intentionally Blank

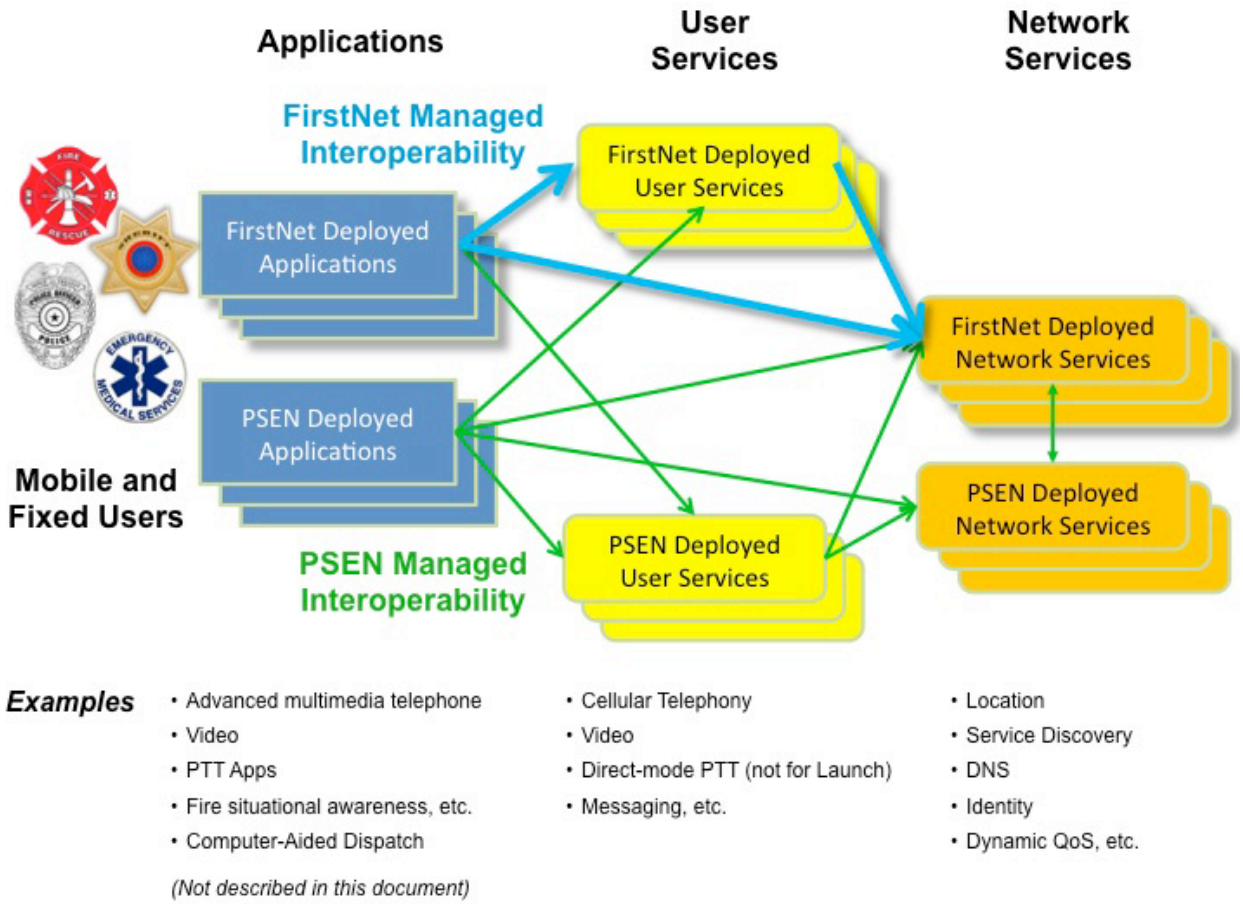
4 Technical Requirements

The NPSBN is a network that contains significantly more than a basic 3GPP LTE system. Traditional LTE Carrier networks provide connectivity from a device to the Internet or the PSTN. The public safety users need the NPSBN to be a complete system that provides nationwide, interoperable applications and services, plus connectivity to their agencies applications. This section is broken down into layers of a system and its design.

4.1 User Services

This section identifies many essential, nationally interoperable services required by users of the NPSBN. While each of these services must be interoperable and accessible across the NPSBN, this section does not provide a complete listing of all public safety user services. Applications provide a set of features and a user interface to an NPSBN-U that may be realized by fixed or mobile devices. User services are logical building blocks of application-layer functionality that application developers may combine to realize NPSBN-U applications. Network Services are building blocks of network functionality, which are provided to applications and user services. Figure 2 illustrates this relationship.

Figure 2. Relationship of NPSBN-Us, Applications, User Services, and Network Services



References:

- Refer to Sections 4.1.5 through 4.1.10 for a description of select FirstNet and PSE-deployed user services.
- Refer to Section 4.2 for a complete description of Network Services.

Figure 2 also suggests that applications, user services, and network services may be deployed by both FirstNet and each PSE. Both FirstNet-deployed and PSE-deployed applications can be *simultaneously* utilized by NPSBN-Us. Further, an application may build upon and utilize user services deployed by either FirstNet or the PSE. The arrows in Figure 2 represent services utilized by an application or user service. While it is anticipated that PSE deployed applications will utilize FirstNet deployed network services, it is not currently anticipated that FirstNet applications will utilize PSE-deployed Network Services.

In this context, "FirstNet Managed Interoperability" is intended to indicate FirstNet will manage and control nationwide interoperability models for FirstNet deployed applications. Similarly, "PSE-Managed Interoperability" is intended to indicate the PSE will manage and control local, tribal, state, and federal interoperability models for PSE-deployed applications.

Today, agencies use specialized applications and user services of their own. FirstNet's role is to enable these specialized user services. This section does not define requirements to enable specialized user services via network services. For example, the Priority and Quality of Service (QoS) network service capabilities (Section 4.3) enable streaming services, such as cellular telephony, voice, and video services.

4.1.1 General User Service Requirements

Following are requirements pertaining to general user service needs on the NPSBN.

Table 20. User Services General Requirements

#	Requirement
1	PSE O&M Users SHALL be able to configure, on a per-user or per-group basis, which applications are authorized for use by the PSE's users. This requirement should apply to all applications, whether deployed by FirstNet, the PSE, or other application hosting entity.

#	Requirement
2	The NPSBN SHALL provide NPSBN-Us the ability to access and use applications (FirstNet-deployed, PSE-deployed, or other application hosting entity) while the NPSBN-U device is using NPSBN or non-NPSBN spectrum (e.g., when the NPSBN-U is roaming to approved roaming partners and technologies). In this context, 'approved roaming partners' means commercial carriers that have an official Service Level Agreement roaming relationship with FirstNet. Using "non-NPSBN spectrum" can occur several ways. For example, LTE-to-LTE roaming or LTE-to-3G roaming. This can also occur for devices with multiple subscriptions (e.g., NPSBN and commercial systems). This requirement may imply different solutions for roaming to commercial 2G, 3G, and 4G technologies.

4.1.2 Logging

Logging refers to the storage of content pertaining to one or more NPSBN-Us. Content can be voice, telemetry (e.g., location), video, and other user traffic. Today, public safety entities use logged content information for a variety of purposes:

- Evidentiary information
- Operations review
- Training

Logging will continue to be a fundamental need for public safety operations on the NPSBN. It should be emphasized that each PSE has different retention and security policies regarding logged content. Therefore, the responsibility of content storage resides with the PSEN. FirstNet must support the ability for agencies to receive a copy of national application content (e.g., a copy of the user's voice, video, data traffic for applications deployed by FirstNet); however there is no expectation that FirstNet should itself store NPSBN-U content.

Following are requirements for logging support in the NPSBN.

Table 21. User Services Logging Requirements

#	Requirement
1	The NPSBN SHALL provide the ability for a PSE O&M User to indicate that a copy of FirstNet-deployed application content involving one of the PSE's users must be transferred to the PSEN. The intent is that the PSE can selectively choose which FirstNet applications will provide logging content to the PSEN. There is no expectation that logging be controllable on a per-user or per-device basis. The PSE should only receive content from the NPSBN for sessions involving one of the PSE's users
2	When indicated by the PSEN, a copy of NPSBN-U content (user traffic, e.g., telephony voice) from FirstNet-deployed applications SHALL be reliably delivered in near real time to the PSEN. The intent is that the content (voice, video, data, telemetry, etc.) not be buffered to disk before transfer. The NPSBN-U must be associated with the PSEN (e.g., part of the agency associated with the PSEN).
3	Encrypted NPSBN application content SHALL NOT be decrypted prior to transfer to the PSEN.
4	The NPSBN SHALL provide a method for an authorized PSE O&M User to obtain key material for encrypted FirstNet application content involving the same PSEN.
5	The NPSBN SHALL prevent logging content from being delivered to a PSEN that does not have one of its users participating in the call or session. The intent is to prevent agency 1 (PSE1) from receiving logged content for users belonging to agency 2 (PSE2), whereby the call/session does not include any responders from agency1.
6	User services provided by the NPSBN SHALL provide a secure interface to the PSEN for the purposes of delivering a copy of NPSBN user service content. The intent is to provide confidentiality and integrity of the content as it is transferred.
7	All content supplied by NPSBN user services to the PSEN for logging SHALL include date, time, time zone, content source device identity, content source user identity, and location of content source (e.g., GPS, eNodeB/cell/sector, state, city, jurisdiction, etc.). The intent of this requirement is for the NPSBN to provide sufficient information for NPSBN application content such that a local PSEN can establish chronology of events (e.g., the NPSBN content may be merged with local PSEN content).
8	The NPSBN SHALL maintain logging usage records identifying which PSE O&M User activated or de-activated the logging service.

4.1.3 Addressing

Addressing refers to the contact information an NPSBN-U uses to initiate communication with another user. Traditionally, a business card lists a telephone number. When that number is dialed, there is an expectation in the commercial cellular world that the person being called will answer the call. Telephone numbers are traditionally associated with a device and not the user using the device (i.e., *Device Addressing*). In other words, there is an implicit assumption of a 1:1 relationship between a device's telephone number and a user in the commercial cellular world. This is not a good assumption for public safety.

Responders may use different devices each day. Different responders may use the same device across shift changes and multiple responders may share some devices during a single shift. For public safety, there exists a one-to-many relationship between a device and the user of the device and this relationship may exist with multiple users simultaneously. This one-to-many relationship complicates addressing because one can no longer count on a device-based address to reach a user. Therefore, public safety requires the additional capability of *User Addressing*. While *Device Addressing* (e.g., telephone numbers) should be retained, additional per-user addressing techniques are also necessary.

While it is desirable to limit complexity and support a single *Device Addressing* scheme for NPSBN-Us, it is not easily achievable. For example, when an NPSBN-U interoperates with the PSTN, she/he may have a telephone number as a device identifier. When this same NPSBN-U device interoperates with LMR PTT, it might have a P25 unit identifier. Therefore, interoperability with other systems will cause a given device to be associated with many device identifiers.

Following are requirements for addressing support in the NPSBN.

Table 22. User Services Addressing Requirements

#	Requirement
1	The NPSBN SHALL support the ability for an NPSBN-U to sign into any device and use all applications the NPSBN-U user is authorized to use. Some devices have a screen and keyboard or other necessary input to support sign-on, but other devices, such as modems, do not. This requirement does not apply to devices without the input capabilities to support sign-on (e.g., a modem). The device is assumed to utilize the NSPBN's common identity framework.
2	Applications deployed by FirstNet SHALL support device addressing.
3	Applications deployed by FirstNet SHALL support user addressing.

#	Requirement
4	For applications deployed by FirstNet, it SHALL be possible for the receiving NPSBN-U to identify the device address of the content/media source. For example, the NPSBN-U should be able to identify the source device of telephone voice or a text message. This requirement may not be readily achievable should the call or session originator be a non-NPSBN-U.
5	For applications deployed by FirstNet, it SHALL be possible for the receiving NPSBN-U to identify the user address of the content source. This requirement may not be readily achievable should the call or session originator be a non-NPSBN-U.
6	For applications deployed by FirstNet, a common User Address format SHOULD be created. The intent is to define a consistent identification format.

4.1.4 Deployment

In many cases, the user services described in this section may be deployed both by FirstNet and PSE O&M Users (e.g., agency information technology staff). Thus, the role of the NPSBN shifts between providing the user service, to enabling a similar user service to be deployed by the PSE. Valid use cases exist for similar user services to be deployed *both* by the NPSBN and the PSEN. For example, an end-to-end secure telephony service might be deployed by a PSE for its NPSBN-Us, whereas FirstNet might deploy a non-secure telephony service to access users outside the NPSBN.

For the user services identified in this section, the following table provides guidance to FirstNet as to which services FirstNet should preferentially deploy and which services FirstNet should enable. When FirstNet is in the role of *enabling* a particular PSEN application, the NPSBN will provide a set of network services (see Section 4.2) to allow PSEN-deployed applications to perform their normal function. Thus, the word *enable* in this context means:

- Do not block or interfere with application performance
- Provide network services (see Section 4.2)
- Provide IP connectivity and transport (see Section 4.3)
- Provide necessary priority and QoS (see Section 6)

Deployment configurations identified with a ‘Yes’ in Table 23 indicate which user services should preferably be supported. A ‘Yes’ in the table further indicates that the minimum user service requirements in the referenced section should be satisfied. User services identified with a ‘No’ are not recommended for the given deployment configuration.

Table 23. Deployment vs. Enablement of User Services by the NPSBN

User Service	Reference	Deployed by FirstNet?	Optionally Deployed by PSE O&M User? (and enabled by FirstNet Network Services)
Telephony	4.1.5	Yes	Yes
NG9-1-1 Emergency Services	4.1.6	Yes	Yes
Commercial Mobile Alert System	4.1.6	Yes	No
Messaging	4.1.8	Yes	Yes
Push-to-Talk Voice	None	No	Yes
Video Services	4.1.9	No	Yes
Status Web Page	4.1.10	Yes (root only)	Yes

Following are requirements concerning deployment and enablement of applications in the NPSBN.

Table 24. User Services Deployment Requirements

#	Requirement
1	As identified in the previous table, FirstNet SHALL provide the identified user services to NPSBN-Us.
2	As identified in the previous table, FirstNet SHALL enable PSE O&M Users to deploy the identified user services.
3	FirstNet and the NPSBN SHALL NOT block or limit the capabilities of any user service deployed by the PSE O&M User. It should be noted that all applications, regardless of which entity deploys the application (e.g., FirstNet or PSE), will operate within the NSPBN's Priority and QoS framework. The intent of this requirement is to enable a PSE to deploy applications suitable for the mission at hand.

4.1.5 Cellular Telephony

The NPSBN can enable Voice-over-IP (VoIP) telephony solutions. For example, the 3GPP standards organization has defined a VoIP solution in Release 9 of their specifications. This is one of a number of open-standard telephony solutions available to the NPSBN.

The major U.S. commercial carriers are not currently providing cellular telephony using LTE 4G technology and are providing cellular telephony service using their 3G infrastructure. Consideration should be given to requiring initial NPSBN smartphone-type devices to be capable of accessing the PSTN through commercial carrier services rather than initially building in the launch of the NPSBN an LTE solution that has not yet been deployed or tested by the carriers.

The 2009 NPSTC 700 MHz Public Safety Broadband Task Force Report and Recommendations [5] identified the "PSTN Voice" feature as a 'desired' application to be supported by the NPSBN:

> *"Public safety 700 MHz voice capable devices such as cell phones, PDAs, or their equivalent shall be capable of placing and receiving full-duplex telephone calls to any telephonic device on the Public Switched Telephone Network (PSTN) in the visited network with the same functionality that cellular telephones operate nationally today. This includes location-based PSAP call routing, E9-1-1 Phase II location transmission, and, if necessary CALEA. In the case where the user transitions into or out of one regional system, the voice session shall be handed off between the two networks with limited loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement."*

Today, the Communications Assistance for Law Enforcement Act (CALEA) is a regulatory requirement supported by commercial carriers to facilitate the capture of user content (including telephony sessions) when a warrant has been issued. The evidence-gathering CALEA capability requires additional equipment and resources in the carrier's network. It is anticipated that FirstNet will have to work with governing officials to determine the applicability of CALEA to the FirstNet network and its subscribers. While compliance with CALEA for public safety users on a private network is not generally required, NPSTC believes that warrant-triggered collection of a secondary user's content will be necessary if FirstNet supports secondary users. However, specific user needs regarding CALEA are not captured in this document.

4.1.5.1 Session Participants

Requirements in this section apply to NPSBN-Us who may or may not be roaming. Following are requirements for session participants in a telephony session.

Table 25. Telephony Session Participant Requirements

#	Requirement
1	The NPSBN SHALL support full-duplex telephone sessions between a mobile NPSBN-U and the PSTN.
2	The NPSBN SHALL support full-duplex telephone sessions between a mobile NPSBN-U and a commercial network user (CN-U).
3	The NPSBN SHOULD support full-duplex telephone sessions to devices.

#	Requirement
4	FirstNet SHALL manage the allocation and assignment of telephony user and device identifiers (e.g., telephone numbers). User and device identifiers are contact addresses that typically show up on a business card.

While standards provide excellent intra-system and inter-system interoperability of telephony services, care must be taken to protect and optionally authorize the type of telephony sessions an NPSBN-U device can support. For example, it may be undesirable for certain NPSBN-U devices to receive telephony calls directly from the public.

Telephony calling restrictions can exist at several levels. For example, should a given PSE be able to receive and/or place calls to the public? Finer-grained calling restrictions might also exist (e.g., the ability to block an NPSBN-U from using 900 numbers).

Following are requirements to control the types of telephony sessions an NPSBN-U may initiate and receive.

Table 26. Telephony Authorization Requirements

#	Requirement
1	The NPSBN SHALL allow authorized PSE O&M Users (e.g., agency information technology staff) to configure which external networks the NPSBN-Ucan initiate telephony sessions with.
2	The NPSBN SHALL allow authorized PSE O&M Users to control which external networks can call the PSE's associated NPSBN-U. The intent, for example, is to control when the general public can directly call an NPSBN-U. External networks are packet or circuit networks connected to the NPSBN. External networks can include, but are not limited to, the Internet, commercial roaming exchange, and the PSTN.
3	The NPSBN SHALL allow authorized PSE O&M Users to block specific telephone numbers and telephone number ranges from being called by the PSE's associated NPSBN-Us. For example, dialing restrictions to prevent 900-number calling.
4	The NPSBN SHALL allow authorized PSE O&M Users to optionally block anonymous or private incoming calls to their associated NPSBN-Us.

Telephony services provide de facto voice interoperability between the widest range of public and private session participants. However, usage of this service may unintentionally disclose NPSBN-U information (e.g., to the public). Services such as "Caller ID" may unintentionally disclose an NPSBN-Us telephone number to the public.

Following are requirements to prevent the unintentional disclosure of NPSBN-U information while using the telephony service. The intent of these requirements is to prevent the NPSBN-U's telephone number and addressing information from being shared under certain circumstances.

Table 27. Telephony Confidentiality Requirements

#	Requirement
1	The NPSBN SHALL allow authorized PSE O&M Users to configure with which networks an NPSBN-U's calling address (e.g., telephone number) is shared. This requirement allows the blocking or sharing of caller ID information on a network-to-network basis based upon the operational desires of the PSE. If the PSE desires to control the sharing of caller ID information on a per network granularity, it is undesirable to require an NPSBN-U, on a per-call basis, to enable or disable "Caller ID Block."
2	The NPSBN SHALL allow authorized PSE O&M Users to configure which NPSBN user classes an NPSBN-U's calling address (e.g., telephone number) is shared. The intent of this requirement, for example, is to prevent the NPSBN-U's telephone number and addressing information from being shared with secondary users on the NPSBN. For example, federal users may only want to share their telephone number with other federal users. 'User classes' can be groupings such as 'primary users', 'secondary users', 'federal users', etc.
3	Should the PSE O&M user block transmission of an NPSBN-U's calling address to another network, user class, or device, the receiving system SHALL be presented with a caller identification of "Unknown."
4	PSE O&M users SHALL have the ability to configure a NPSBN-U such that a per call block, will block all data being sent regardless of network or user class.
5	The NPSBN SHALL provide confidentiality for all VoIP signaling traffic from the NPSBN-U device to the telephony application server. The intent is that signaling information for an NPSBN-U's telephony session not be viewable while in transit; especially when the NPSBN-U is roaming outside the NPSBN.
6	For telephony calls between two or more NPSBN-Us homed to the NPSBN (i.e., NPSBN subscribers), it SHALL be possible for the originating NPSBN-U to choose end-to-end encryption of a voice conversation on a per-call basis. In this context, end-to-end means from the source device to the destination device(s) in the NPSBN network. Encryption on an end-to-end basis will likely require both end devices to support the desired encryption.

As telephony service has evolved over the past several decades, numerous supplemental calling features have been developed. FirstNet should provide services equivalent to those provided by commercial carriers. VoIP technology enables even further supplemental capabilities.

Call monitoring (discrete listening) by, e.g., dispatchers, for telephony service should be considered. This should not be confused with CALEA and is intended to mirror the PTT call monitoring capabilities today. The need for this telephony-based capability is unclear, however telephony may be subject to state and federal restrictions on call recording. This topic should be explored in the future.

Following are requirements for supplemental telephony calling features.

Table 28. Telephony Calling Features Requirements

#	Requirement
1	The NPSBN shall support the transmission of telephony caller addressing information (e.g., “Caller ID”).
2	On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the transmission of caller addressing information (e.g., “Caller ID”).
3	On a per-user basis, the NPSBN SHALL provide the ability for an NPSBN-U to enable or disable the per-call transmission of caller addressing information (e.g., “Caller ID Block”).
4	The NPSBN shall support telephony voicemail service.
5	On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the use of voicemail service.
6	The voicemail service SHALL support a per-user passcode, which must be entered by the NPSBN-U prior to the management of voicemail message.
7	Voicemail content that is stored SHALL be encrypted to prevent unauthorized recovery of the content. The intent is to prevent interception of the content when a hard disk, for example, is removed from the voicemail system.
8	The NPSBN SHALL support telephony call conferencing.
9	On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the use of call conferencing by the NPSBN-U. In this context, a call conference includes three or more participants.
10	The telephony service SHALL support the creation and use of dialing plans using short-address numbers. The intent is to allow NPSBN-Us in the same PSE to call one another using PSE-specific short addresses (e.g., “123” dials the chief of police).
11	It SHALL be possible for an authorized PSE O&M User to define an extension for an NPSBN-U or device.
12	The telephone service SHALL support toll (or better) audio quality.

The IP-based technologies comprising the NPSBN enable advanced interoperation of applications. Following are telephony requirements for interoperability.

Table 29. Telephony Interoperability Requirements

#	Requirement
1	The NPSBN SHALL provide the ability for an authorized PSE O&M User to selectively join an NPSBN telephony session with an LMR or broadband voice session. Patching capabilities are a commonly used feature today. The intent is to allow a full-duplex telephony call to be interworked with a broadband call.

4.1.6 NG9-1-1 Services

Next-Generation 9-1-1 (NG9-1-1) uses IP technology to initiate emergency sessions via a number of means, including telephony and messaging. A variety of content (i.e., user media, such as video clips and pictures) can also be provided to the NG9-1-1 PSAP. Appropriate NG9-1-1 content can be delivered to dispatchers from the PSAP call-taker

It is envisioned by multiple stakeholders (including commercial operators, NENA, and APCO) that the network supporting NG9-1-1, also known as an Emergency Services IP Network or ESINet, and the NPSBN Core (both wired broadband based) could potentially be parts of one and the same network (or the same network of networks).

Future public safety networks should support advancements in infrastructure and device location technologies, as that of other location technologies described in Section 4.7.3.8.

Following are requirements for NG9-1-1 service.

Table 30. NG9-1-1 Service Requirements

#	Requirement
1	After originating the NG9-1-1 session, NPSBN-Us SHALL be able to send to and receive from the local PSAP's NG9-1-1 system, emergency text messaging.
2	After originating the NG9-1-1 session, NPSBN-Us SHALL be able to send to and receive from the local PSAP's NG9-1-1 system, images, audio clips, and video streams.
3	After originating the NG9-1-1 call, NPSBN-Us SHALL be able to send to and receive from the local PSAP's NG9-1-1 system, full-duplex telephony sessions.
4	For each NG9-1-1 session origination, the NPSBN SHALL determine the originating NPSBN-U's location and deliver this information to the PSAP. The intent is for the NPSBN to support both device-based and infrastructure-based location determination techniques.

4.1.7 Commercial Mobile Alert System (CMAS) Services

The Commercial Mobile Alert System (CMAS) is part of the Integrated Public Alert and Warning System (IPAWS) that allows designated government entities to deliver warning notifications (alerts) to commercial wireless users. CMAS is defined by the FCC's First, Second, and Third Report and Order in the "Matter of the Commercial Mobile Alert System" [6] as an optional service allowing the commercial wireless operators to voluntarily comply and provide CMAS services to their subscribers.

The CMAS network allows the Federal Emergency Management Agency (FEMA) to aggregate alerts from different sources and send them over a secure interface to participating wireless service providers who in turn will send these emergency alerts as text messages to their subscribers.

CMAS defines three classes of warning notification: Presidential, Imminent Threat, and Child Abduction Emergency (AMBER alert). The warning notifications are distributed to a notification area specified by the warning notification provider.

4.1.7.1 CMAS Requirements

Following are high-level requirements for CMAS service.

Table 31. CMAS Requirements

#	Requirement
1	The NPSBN SHALL be able to receive CMAS alerts from the CMAS Federal Alert Gateway.
2	The NPSBN SHALL support all three categories of CMAS alerts: Presidential, Imminent Threat, and Child Abduction/AMBER alerts.
3	All NPSBN-U SHALL be able to receive CMAS text alerts using CMAS-capable UE that can present the alert.
4	All NPSBN-Us SHALL be able to receive CMAS text alerts using CMAS-capable UE that can present the alert.
5	NPSBN-Us SHOULD be allowed to opt-out of the presentation of specific alerts that are not Presidential alerts.
6	The NPSBN SHALL support the periodic testing of CMAS service as defined by the FCC.

4.1.8 Messaging

This section describes functional requirements for text and multimedia messaging, as well as related security and interoperability functionalities public safety needs.

The 2009 NPSTC 700 MHz Public Safety Broadband Task Force Report and Recommendations [5] provided a messaging-related usage scenario describing some basic public safety messaging needs. The quote describing this scenario appears below:

> *"A Public Safety user arrives on a visited network while responding for mutual aid for disaster recovery. She is able to receive text messages providing status updates on staging locations and voice radio assignments. Once on the scene, she is able to take photographs of damaged infrastructure and send them to the local EOC. She also exchanges multimedia messages with support staff who use commercial cellular phones on commercial networks run by various carriers."*

The above scenario suggests the need for messaging capabilities, which are captured in the requirements tables that follow.

Note that in this section, terms such as *text messaging*, *multimedia messaging*, and *messaging service* represent user-visible capabilities presented by UE devices. The underlying technology by which these capabilities might be implemented is not considered in this discussion. As such, any references to specific implementation technologies in this section are used for illustrative purposes only.

4.1.8.1 Messaging General Requirements

This section captures the most basic capabilities required of the messaging service. Following are general requirements for messaging.

Table 32. Messaging General Requirements

#	Requirement
1	NPSBN-Us SHALL have the capability to send and receive text messages to and from other NPSBN-Us and CN-Us.
2	NPSBN-Us SHALL have the capability to send text messages addressed to a group of NPSBN-Us.
3	NPSBN-Us SHALL have the capability to send and receive multimedia messages to and from other NPSBN-Us.
4	NPSBN-Us SHALL have the capability to send multimedia messages addressed to a group of NPSBN-Us.

4.1.8.2 Messaging Interoperability Requirements

This section captures messaging service interoperability needs. Following are interoperability requirements for messaging.

Table 33. Messaging Interoperability Requirements

#	Requirement
1	The messaging service SHALL provide a standard mechanism to provide interoperability with PSEN email systems. The intention is for the messaging service to provide a standard mechanism (e.g., SMTP) to allow for message interoperability with PSEN email systems as opposed to supporting many such interfaces.
2	The messaging service SHALL provide the ability for suitably authenticated and authorized users to send and receive text messages to and from NPSBN-Us using Status Web Pages[13] via the public Internet. The intention is to provide text-messaging capability for suitably authorized public safety personnel (e.g., wired users) to contact NPSBN-Us via the public Internet.
3	The messaging service SHALL provide the ability for suitably authenticated and authorized users to send and receive multimedia messages to and from NPSBN-Us using Status Web Pages[13] via the public Internet. The intention is to provide multimedia-messaging capability for suitably authorized public safety personnel (e.g., wired users) to contact NPSBN-Us via the public Internet.

4.1.8.3 Other Public Safety Messaging Requirements

The NPSTC Public Safety Communications Report, "Use Cases & Requirements for Public Safety Multimedia Emergency Services (MMES) Rev B, May 2012" [7], provides additional requirements for public safety multimedia messaging. The report describes capabilities that build upon concepts associated with NG9-1-1 for public safety emergency and non-emergency text and multimedia messaging. See also Section 4.1.6 for requirements associated with NG9-1-1 messaging.

4.1.9 Video Services

The use of video technology by public safety is extensive, and is expected to grow significantly over the next 10 years. NPSTC's Public Safety Communications Assessment 2012 – 2022, June 5, 2012 [8], explored numerous video needs. The following text is referenced from NPSTC's June 2012 assessment:

> *"Incident command staff and supervisors identified the need to access vehicle-mounted video cameras in fire/rescue and law enforcement vehicles on an as-needed basis (versus a continual video feed). The video feed would allow command post and Emergency Operations Center (EOC) personnel to visualize the incident scene in relation to damage and apparent needs when compared to other incident scenes. Vehicle-mounted video also enhances on-scene safety by allowing third parties to check on the incident scene, verify that personnel are accounted for, and monitor the success or failure of the incident mitigation plan. Vehicle-mounted video also allows the Incident Command team to "see" the incident and develop a better perspective of the operational requirements. In the absence of video, the command staff must rely on a radio transmission description of the scene from first arriving units."*

Nearly all current video applications are localized. That is, the source cameras and responders using the video information are localized to the areas they serve. While video is not typically sourced from one location across the country, video is more often shared between responding agencies (PSEs) for a given incident.

The NPSTC Video Quality in Public Safety (VQiPS) group is investigating methods to define and quantify public safety video. For example, tactical video may be determined to require a given CODEC, frame rate, resolution, etc. This section will not focus on those application-specific CODECs and parameters. It is understood that CODEC technology will evolve over time, potentially altering the parameters (bandwidth, latency, packet loss) used by the NPBSN.

The NPSBN only "sees" attributes such as bandwidth, latency, packet loss, etc. These attributes should be taken advantage of as the system is built out over time. However, in concentrating on what is critical for launch, the requirements in this section focus on the ability of the NPSBN to provide functionality for one or more PSENs to stream video traffic in real-time to one or more other PSENs.

This section focuses on two primary sets of needs for NPSBN-Us:

- The NPSBN enabling PSEN-deployed video applications
- NPSBN-deployed video services

Following are requirements for the NPSBN to enable local PSEN video applications.

Table 34. NPSBN Enabling PSEN-Deployed Video Requirements

#	Requirement
1	The NPSBN SHALL support the ability for a PSEN to deploy one or more video applications.
2	The NPSBN SHALL provide the ability for one or more PSENs to stream video traffic in real-time to one or more other PSENs. The intent is to support the sharing of fixed and mobile video assets between PSEs.
3	The NPSBN SHALL provide the ability for NPSBN-Us belonging to different PSENs to exchange real-time video streams from a PSEN-deployed video service.

The previous table focused on the NPSBN's role in enabling PSEN-deployed video applications. Table 35 turns to video applications optionally deployed by FirstNet. When FirstNet eventually deploys applications such as telephony and push-to-talk, real-time video streams are viewed as optional supplemental streams for these sessions.

Following are requirements for FirstNet-deployed video sessions.

Table 35. NPSBN-Deployed Video Requirements

#	Requirement
1	The NPSBN SHALL provide the ability for one or more NPSBN-Us to stream video traffic in real-time to one or more other NPSBN-Us using the NSPBN video service.
2	The NPSBN SHALL support the ability to interface with fixed video sources (including third-party systems), such as facility security cameras.

4.1.10 Status Web Page

The 2009 NPSTC 700 MHz Public Safety Broadband Task Force Report and Recommendations [5] identified the "Status/Information Home Page" as a 'required' application to be supported by the NPSBN:

> *"Public safety or public/private partnership network operators shall provide a universal method to obtain a home page for visitors to the system. This home page will facilitate access to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with visitors to the system."*

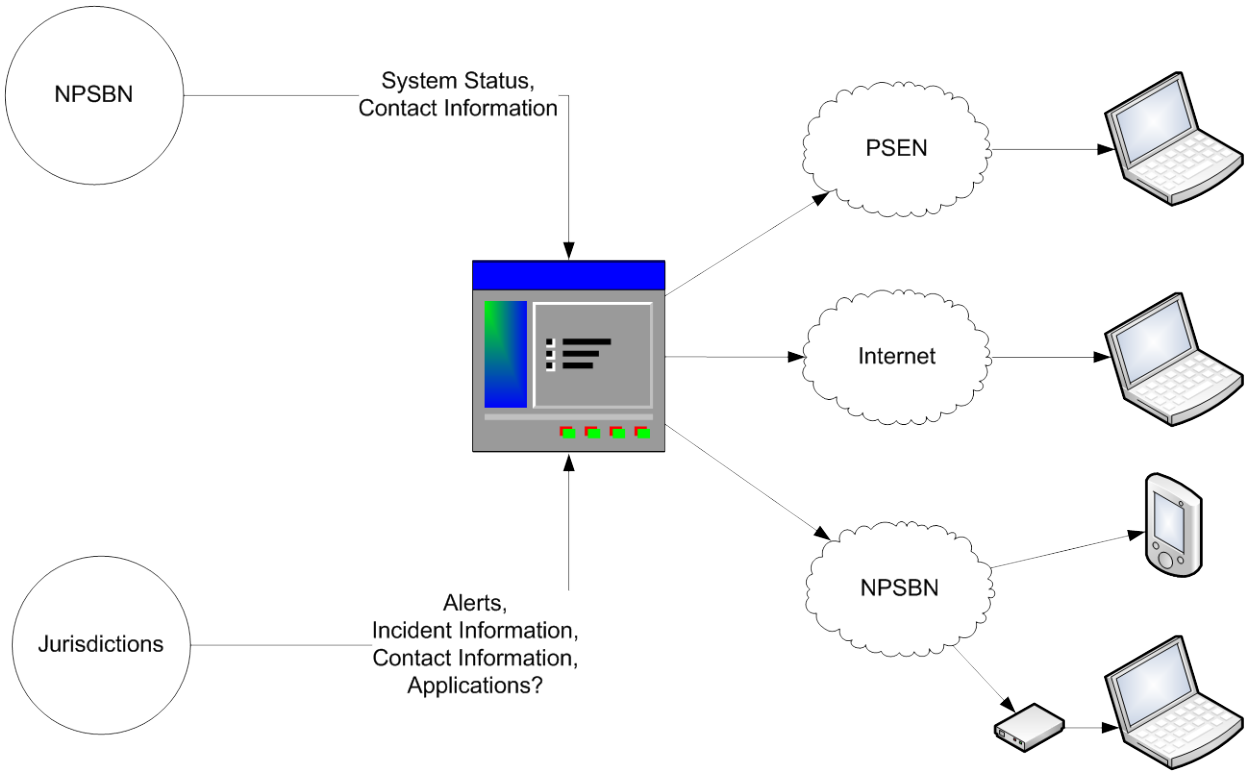
The same document expanded on the definition of this capability:

> *"Users visiting a network will need a simple and universal way to obtain basic information. The method for reaching this home page should be straightforward and the same across networks. Some information may be on a need-to-know basis and should be protected by credentials issued to the visitor. As new incidents develop, network operators may re-capture users for updates."*

This section will hereafter refer to "Status/Information Home Pages" as "Status Web Pages." The term "visitor" is interpreted to mean an NPSBN-U who has traveled to or is en route to a particular area, which may or may not be within the NPSBN-U's home jurisdictional area and who is authorized to access a given Status Web Page.

As Figure 3 illustrates, each Status Web Page instance receives relevant information from the NPSBN and one or more PSENs. In turn, this information is made available to other authorized PSENs, Internet users (e.g., public mission specialists, the press, etc.), and NPSBN-Us.

Figure 3. Status Web Page Concept Diagram



4.1.10.1 Accessing Status Web Pages

The primary use case envisioned for accessing each Status Web Page at launch is:

- A responder wishes to obtain relevant operational information relative to their current position (e.g., what incidents are taking place in the immediate area?).

Future development of the Status Web Pages should include:

- A responder wishes to become informed about operational status regarding a specific location (e.g., the responder wishes to become briefed on the incident prior to arriving on-scene).
- A responder wishes to become informed about network status relative to their current position, and/or regarding a specific location.

Different types of agencies may wish to deploy their own Status Web Page instances. For example, federal users may wish to have their own Status Web Page, which only federal users may access. This capability, while desirable over the long term, is not considered critical for launch.

Following are requirements for accessing the Status Web Page.

Table 36. Accessing Status Web Page Requirements

#	Requirement
1	The information content of NPSBN Status Web Pages SHALL be accessible for both reading and writing by applications.
2	Prior to accessing privileged Status Web Page information, an NPSBN-U or application SHALL be authenticated. The term “NPSBN-U” in this requirement is intended to mean the human being’s credentials, rather than the device’s credentials to use the NPSBN.
3	The NPSBN SHALL allow an NPSBN-U or application to access the Status Web Pages relevant to the NPSBN-U’s current location and function. The assumption is that the NPSBN-U is not required to know a specific address for a web page, given their location. Rather, a relative URL scheme (for example, https://local.police.gov) should be used. It should be noted that there might be many Status Web Pages governing a given area, which are differentiated by the NPSBN-U’s function (e.g., police, fire, EMS, federal, etc.).
4	An authenticated NPSBN-U or application SHALL be able to access any Status Web Page from the Internet, PSEN, PSAP, or other IP network external to the NPSBN.

4.1.10.2 Status Web Page Content

The Status Web Page application is one of the key applications that differentiates commercial broadband networks from the NPSBN. Status Web Pages are required at launch and they will continue to evolve as different network use cases are developed and adopted. Status Web Pages will provide public safety with basic and enhanced situational awareness. Status Web Pages will assist responders in more effectively performing their normal function and allow agencies to work together more effectively through mutual aid. It is key that they evolve as the NPSBN evolves.

As one of the key applications which enable basic functionality of the NPSBN, the authors believe that a thorough detailed requirements collection process must be followed using industry standard software development and life cycle management processes to effectively design the Status Web Page application. As previously articulated, the Status Web Page is a key application that makes the NPSBN functionally different from commercial broadband services. The authors believe that FirstNet should begin the process of application definition and design immediately. Any attempt to include detailed requirements for the content of the Status Web Page in this document could have potential damaging results on the application development process.

For the Status Web Pages to be useful, information pertinent to the responder’s location and function must be provided. Thus, Status Web Pages must be adaptable based on the user’s current role, function, and location. Because the Status Web Pages are anticipated to contain sensitive incident information, access to this information must be carefully controlled.

The Status Web Page content will eventually need to be adaptable based on the NPSBN-U's current role, function, and location.

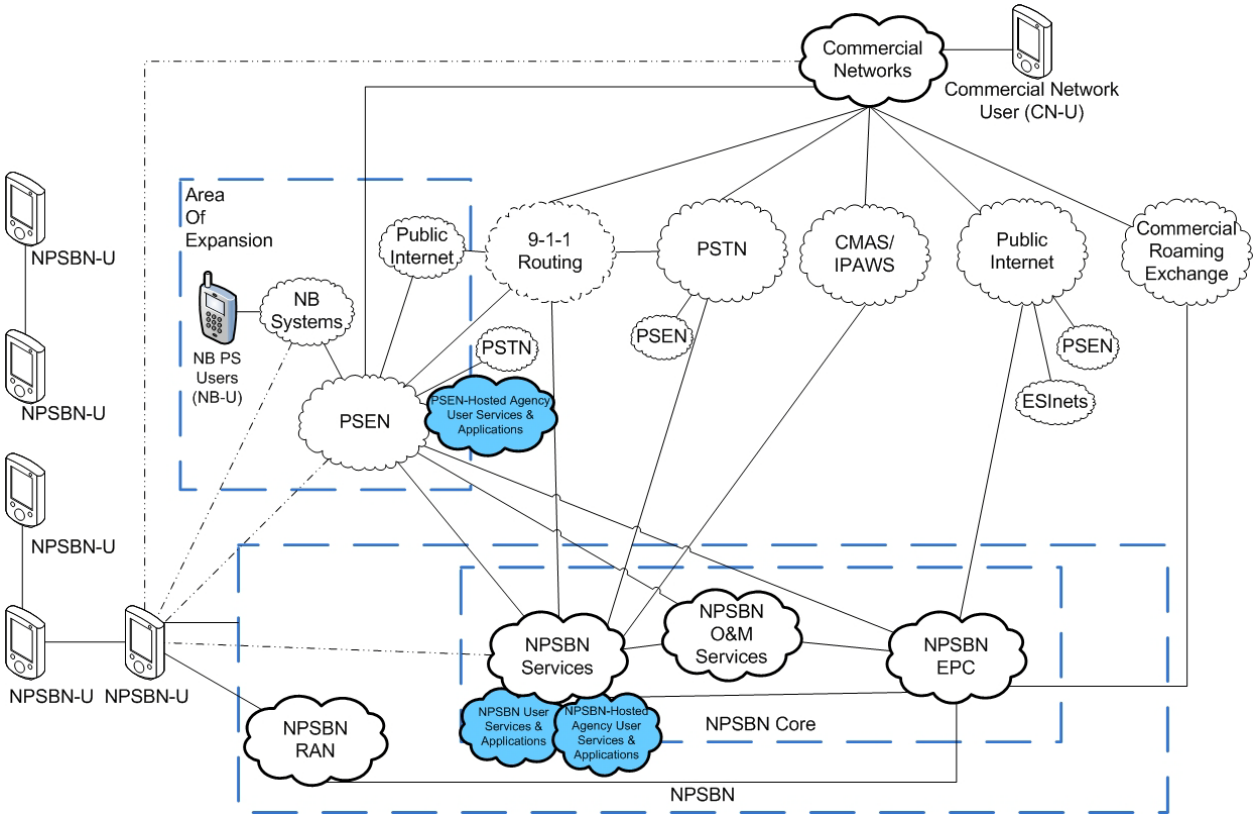
Dispatchers, CAD operators, and in-field responders are all envisioned to require the ability to post operational information to a given Status Web Page. While the enhanced capabilities of the future system are beyond the scope of launch requirements, it is important to note that the Status Web Page system should be designed with future needs in mind.

4.1.11 Hosted Applications

This section provides requirements to support the expansion and growth of applications hosted within the NPSBN. FirstNet, the PSENs, or vendors could provide these applications. The NPSBN could create an environment to enable new applications and encourage a robust applications ecosystem by providing the platforms to host application servers, by providing UE device applications, and by providing an applications distribution platform.

Applications hosted on the NPSBN can be provided either by the NPSBN, PSENs, or vendors. Figure 4 shows hosting locations shaded in blue.

Figure 4. Application Hosting Locations



4.1.11.1 Application Hosting

The NPBSN will be well-positioned to host FirstNet-, PSEN-, and vendor-supplied application servers. FirstNet could host applications for access to common or interoperability services. PSENs could host their applications on the NPSBN rather than in their home networks for applications. The NPSBN could provide vendors the ability to quickly deploy solutions to PSENs that sign on to vendor-supplied application servers.

Should the NPSBN host applications, careful analysis and planning is required of the backhaul, transport, security, and network subsystems. Attributes such as bandwidth, latency, cost, loading, and availability should be carefully studied so as to not impact primary NPSBN functions.

Following are general hosting requirements for the NPSBN.

Table 37. General Hosting Requirements

#	Requirement
1	The NPSBN SHOULD provide application hosting capabilities within the NPSBN.
2	PSEs SHALL NOT be required to host applications within the NPSBN Services.
3	PSEs SHALL be able to locally host applications within the agency PSEN.
4	The NPSBN SHOULD provide a service hosting platform as a service to PSENs.
5	The NPSBN SHALL provide the ability for PSEs to remotely manage their applications.
6	The NPSBN SHOULD provide a service hosting platform as a service to vendors.
7	The NPSBN SHALL provide the ability for vendors to remotely manage their applications.

4.1.11.2 Application Distribution and Management

This section outlines the requirements for a secure method of deploying applications to NPSBN-Us. The applications include FirstNet-, PSEN-, and vendor-provided applications both NPSBN hosted and locally hosted. The NPSBN application distribution and management service allows PSENs to efficiently manage their users' applications. This capability is not meant to prohibit or interfere with the direct loading of applications onto the UE devices of NPSBN-Us by PSE administrators; rather the application distribution and management service is an option for agencies to adopt if desired.

Once UE devices connect to the NPSBN, the application distribution and management service provides mechanisms for applications to be installed, upgraded, and removed from UE devices. This service should be accessible both from the network and locally on the device. A notification service should be available to provide an indication to the user when an application or upgrade is available. The service should also be capable of limiting certain applications or upgrades from being installed on particular devices. Authorized entities, such as PSE administrators, and application owners will have control over

what users can access the system and to what extent they can access applications. This should be able to be restricted by user and by applications, in addition to denying access to the service altogether.

Some types of applications will likely be shared among most of the devices in the network, such as anti-virus applications. Others might be dependent on the UE device's NPSBN-U, such as NCIC database access for police officers or medical records for EMS personnel. The application distribution and management service shall restrict the access of some applications based on the user of the device. The service shall also be capable of pushing required applications and updates to a device when a particular user logs on to the device.

Following are requirements for UE device application distribution and management.

Table 38. Application Distribution Platform Requirements

#	Requirement
1	The NPSBN SHALL provide an application distribution and management service for NPSBN-U applications.

4.2 Network Services

This section describes launch day requirements for NPSBN network services, such as location-based services, Domain Name System (DNS) services, device management services, and an identity management framework. These services can be provided by a central authority in support of NPSBN-Us, delivered through either centralized or distributed service mechanisms. In addition, there are significant security requirements to consider at the network services layer, which this section discusses.

Figure 5 highlights the network services portion of the revised reference model for the NPSBN, which is the core of the NPSBN reference architecture. The NPSBN core constitutes the NPSBN services and O&M services and provides interfaces to the various PSENs.

4.2.1 Location Services

This section describes functional requirements around the network assisting UEs to locate themselves, PSEN applications locating UEs, or network management location support.

Location services provide a unique opportunity to support public safety response and operations. By querying the network of location enabled UEs an Incident Commander can locate resources, calculate, and direct responding units without the need to speak.

In addition, location services are necessary for general health, maintenance, and configuration of devices at the control and signaling layer. These requirements cover some of the considerations related to this type of information including security requirements.

The NPSBN will need to provide a mechanism that allows applications and services to access the presence, function, location, and availability of NPSBN-U. The opportunity to exploit UE location data when it is associated with the UE unique identifiers poses a security threat. To protect this data, the following needs to be addressed:

- Location data on the UE, whether for user applications or network support when stored on the UE, needs to be protected.
- Protection of location information when associated with the UE unique identifiers and transported from the UE to applications or network management services.
- If the historical location information along with the UE unique identifiers is to be stored, this data can be controlled and access limited to approved personnel.
- Location information, date, time, and unique identifier typically are not stored by network services except for network management purposes the retention time are limited.
- PSE can have the ability to set the policy that would allow a UE to restrict access to its location information.
- UEs can have the ability to turn off location services on individual devices if the policy is allowed by the PSE.
- Historical location data which includes unique identifiers, location, date, and time can have appropriate record retention rules established by the owner of the information, i.e., PSE, FirstNet, or federal agencies.

Following are requirements for location services.

Table 39. Location Services Requirements

#	Requirement
1	The NPSBN SHALL provide the ability for UE devices to report location information to the network for device management and configuration purposes.
2	The NPSBN SHALL limit access to UE device location information based on PSE policies.
3	The NPSBN SHALL provide an application location service that stores UE locations tied to user ID for purposes of applications requiring locations.
4	The information called Location Information SHOULD at a minimum include geographical location, time, date, and a unique identifier.
5	The Location Information applications SHALL control and protect the data provided by network management services if that data is being stored on the device or by PSEN applications.
6	The Location Information applications SHALL control and protect the data provided UE applications if that data is being stored on the device or by PSEN applications.

#	Requirement
7	The network management service SHOULD allow an authorized entity to retrieve a particular UE's previous geographic location over some agreed upon range of time.
8	The network management service SHALL allow an authorized entity to retrieve a particular UE's current network location (RAN, eNodeB).
9	The device management service SHALL allow an authorized entity to retrieve a particular UE's previous network location (RAN, eNodeB) over some agreed upon range of time.
10	The NPSBN SHALL provide a presence service.
11	The NPSBN presence service SHALL provide interface specifications for use by other application servers.

4.2.2 Responder Emergency

Similar to an emergency button on today's LMR radios, activation of this capability provides heightened priority and QoS to the NPSBN-U, but also notifies dispatchers and other appropriate personnel of the life-threatening condition. Because the NPSBN service supports more than basic data and voice from LMR, the definition of Responder Emergency must account for all applications, including video.

Responder Emergency includes:

- Provision of standard mechanisms to activate and clear a Responder Emergency by the responder's UE, by a third party via UE (such as a field command tablet), and by third party via a back-end application (such as a dispatch terminal). It should be noted that in some cases, it is not desirable for the responder to be able to clear their own emergency condition.
- Ability for a responder's agency to define the applications used when one of the agency's responders activates the Responder Emergency capability.
- Activation of the Responder Emergency function provides the highest ARP priority level for emergency applications.
- When activated, Responder Emergency preempts other lower-priority applications on the NPSBN if necessary, in order to obtain resources. Applications used when the Responder Emergency function is activated are prohibited from being preempted.

Following are requirements for the Responder Emergency capability.

Table 40. Responder Emergency Requirements

#	Requirement
1	The NPSBN SHALL provide the ability for the NPSBN-U (or other authorized user) to indicate and clear an emergency condition. When initiated, the agency-defined list of emergency applications SHALL be given the highest NPSBN priority and may pre-empt, if necessary, other resources to be admitted.
2	When the Responder Emergency function is initiated, an agency-defined list of applications SHALL be given the highest NPSBN priority and may pre-empt, if necessary, other resources to be admitted.
3	An authorized PSEN administrator SHALL be able to configure which NPSBN-Us can initiate and clear the emergency condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the emergency condition.

4.2.3 Immediate Peril

Because all application types (e.g., voice, video, data, etc.) share a single set of LTE resources (e.g., over-the-air resources), this presents public safety with a new problem not present in LMR systems. A static (default) ordering of application types typically de-prioritizes video and other high-bandwidth applications. This creates a strong lack of flexibility in the framework and likely would prevent video from becoming mission critical. The user community indicated that, by default, video service would be pre-empted from a congested cell before other applications (see Section 4.2.2). Without ability for an NPSBN-U to override the default admission priority for video service (and other lower priority applications), NPSBN-Us can never count on the application to be available in a congested NPSBN cell.

To address these needs, NPSTC's Priority and QoS Task Group defined user requirements [4] for a prioritization feature that allows a normally de-prioritized application to be "re-prioritized" by the NPSBN for an authorized NPSBN-U, in the event of an imminent threat to human life. For example, a responder that must relay video to the incident commander to inform her that the fire has spread dangerously close to a tanker truck would use Immediate Peril.

Immediate peril includes:

- Provision of a standard mechanism to activate and clear Immediate Peril by the responder's UE, by a third party via UE (such as a field command tablet), and by a third party via a back-end application (such as a dispatch terminal). It should be noted that in some cases, it is not desirable for the responder to be able to clear their own immediate peril condition.
- Ability for the entity initiating the Immediate Peril condition to be able to select the applications to receive heightened ARP priority level.

- The ability to utilize both the Responder Emergency and Immediate Peril capabilities from the NPSBN-U (non-concurrent).

Following are requirements for the Immediate Peril capability.

Table 41. Immediate Peril Requirements

#	Requirement
1	The NPSBN SHALL provide the ability for the NPSBN-U (or other authorized user) to initiate and clear the Immediate Peril condition.
2	When the Immediate Peril condition is initiated, the end-user-selected applications SHALL be given elevated NPSBN priority. The exact elevated priority given to an application with Immediate Peril priority is a policy decision to be determined by the PSEN.
3	An authorized PSEN administrator SHALL be able to configure which NPSBN-Us can initiate and clear the immediate peril condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the immediate peril condition.

4.2.4 ICS Incident Priority

In an effort to improve mutual aid and the overall ability for responders to work together, the National Incident Management System (NIMS) was developed by DHS and issued in 2004. A best practice that was incorporated into NIMS was the Incident Command System (ICS). ICS is a nationally standardized incident organizational structure for on-scene management of all-hazards incidents. It incorporates a Unified Command (UC) approach, whereby individuals designated by their jurisdictional authorities jointly determine objectives, plans, and priorities and work together to execute them. ICS is commonly used today for incident command and control. Key elements of ICS are 1) standardized incident classification, and 2) standardized roles within a given incident organizational chart.

NPSTC's Priority and QoS Task Group [4] determined a linkage between standard ICS management practices and standard LTE priority and QoS was needed. In effect, this linkage provides public safety with needed per-incident prioritization capabilities. Without this capability, the NPSBN will be unable to distinguish resources for a four-alarm fire from a minor traffic accident.

In some incidents, Computer Aided Dispatch (CAD) performs the initial incident classification. Once the Incident Commander (IC) or his designee arrives on-scene, a formal incident classification is made. Once this classification is made, an association with NPSBN priority and QoS can be made.

ICS Incident Priority includes:

- The ability to alter an NPSBN-U's priority and QoS based on the ICS type of incident.

- The ability to alter an NPSBN-U's priority and QoS based on the NPSBN-U's ICS role.
- Assignment of an NPSBN-U to a specific ICS incident and role.

Following are requirements for the ICS Incident Priority capability.

Table 42. ICS Incident Priority Requirements

#	Requirement
1	The NPSBN SHALL allow an NPSBN-U's priority and QoS to be altered dynamically based on the Incident and locally defined needs.

4.2.5 Fundamental Network Services

4.2.5.1 Domain Name Services (DNS)

This section describes requirements supporting the ability to locate a particular network system or service by name. Domain Name System (DNS) is an Internet Engineering Task Force (IETF) standard service, which helps users to find their way around the Internet.

DNS is susceptible to the same types of vulnerabilities as any other distributed computing system. Conventional network-level attacks such as masquerading and message altering, as well as violations of the integrity of the hosted and disseminated data, can result in adverse impacts to users. Fake DNS information provided by a masquerader or intruder could direct an unsuspicious user not to the server or service they intended to go to, but to one that can infect and compromise a UE resulting in the theft of confidential information. Separation of DNS services from the public Internet will also add protection from cyber security exploits currently affecting publically accessible DNS servers, which will ensure that UEs can quickly and confidently connect to systems providing them critically needed data and communications. Implementing secure DNS also helps to defend against these types of issues by enabling UEs to detect bogus DNS replies.

To provide both robustness and security for both the NPSBN and the PSEN, FirstNet-provided DNS services can be divided into at minimum three separate planes: 1) FirstNet EPN Core Services, 2) Roaming Core Services, and 3) Public Safety Agency services with Top Level Domain DNS Servers for each plane housed in a secure facility in a trusted DMZ zone and utilize DNSSec aligning with OMB Memo M-08-23 [9].

While the following requirements are DNS focused and rather technical in nature, when implemented in concert, they will provide public safety FirstNet users with a robust and resilient name resolution system ensuring they have dependable and swift access to the critical information they require.

Table 43. Domain Name Services Requirements

#	Requirement
1	The NPSBN SHALL provide robust and geographically dispersed, load balanced, and redundant DNS services initially for the NPSBN and eventually for both the NPSBN and PSEN, ensuring users have DNS service to their UEs that are reliable, responsive, resilient, and centrally monitored with ability to resolve entries including PSEN, network services, and user service.
2	These DNS services, when provided, SHALL also be accessible from other public safety networks such as PSAPs.
3	PSEs SHALL be actively notified of planned future changes in advance that may adversely affect their use of the network.
4	PSEs SHOULD have a voice in approving DNS changes made to the NPSBN that have potential to adversely affect them.
5	DNS services SHALL be deployed in such a manner to ensure resiliency, failover, ease of maintenance, and consistent high performance, and minimize backhaul traffic.
6	To allow for nimble recovery from NSPBN system failures and ensure public safety users with a simple roaming experience, DNS server IP addresses SHOULD NOT be hard coded in an individual UE.
7	The NPSBNMUST put in place a system to ensure IP addresses across the entire national level of the FirstNet system are unique.
8	To ensure high reliability for common critical infrastructure across the system, automated DNS zone transfers SHALL be implemented for only non-critical functions and systems.
9	To ensure high availability, updates to DNS entries that are critical to the stable operation of the system SHALL be done via pre-approved, pre-scheduled change control, and be closely supervised except when resolving a catastrophic system failure where time is of the essence.

4.2.5.2 Network Time Service

A trusted time source is required for the NPSBN as a fundamental service to infrastructure, operations, and users. The NPSBN system will need a trusted network time source for internal time synchronization between infrastructure network elements as well as to provide accurate time for the users of the network. As such the NPSBN must make available trusted time services internally as well as to the end user of the system. Following are requirements for time service.

Table 44. Time Service Requirements

#	Requirement
1	The NPSBN SHALL provide a network time service available to NPSBN infrastructure.

#	Requirement
2	The NPSBN SHALL provide a network time service available to mobile users of the network.

4.2.6 Service Discovery

Commercial networks operators have deployed service delivery frameworks (SDF) to simplify the creation and delivery of new applications and services to their networks. The NPSBN should have a similar set of processes and mechanisms to provide access to applications and services with the added focus on the security of the applications and authorized access mechanisms based on the identity of the user. The immediate impact of an SDF on users will be to provide for operational processes to access applications by users without requiring any particular knowledge of backend systems such as billing, location services, authentication, etc. The SDF will allow application developers to easily build into their applications any necessary services provided by the NPSBN and carry with it important aspects of the NPSBN such as QoS characteristics.

A very simple example is a developer builds an application that accesses the NPSBN location services in order to put an image of a user and his peers on a map for purposes of information exchange during a public safety event. The SDF provides the interface specification to the location service so that the developer can easily access the service provided by the NPSBN. The user by running the application is given the benefit of the location service without needing any particular knowledge of the service. This SDF should allow local PSENs, third-party developers, and agencies to access the provided services through common well-defined interfaces. In addition to providing access to existing NPSBN common services, the SDF will allow localities and agencies to use the SDF to publish services they want to make available to either their local audience or to a broader audience. The SDF will also provide interfaces for the delivery of applications to users through both a push and pull mechanism. PSEN agencies can push applications and services to its users through the interfaces provided by the SDF, and users can pull applications and services from a repository that uses the SDF interfaces to create an application repository exposing to users the available applications and services.

The concept of a service delivery framework has developed over time to become a standard deployment feature for wireless network operators. Oftentimes service delivery framework, service delivery platform, and even service-oriented architecture are used interchangeably. However the relationship of these terms will be the following for this discussion:

- **Service delivery framework (SDF)** – A set of principles, standards, policies, and constraints used to guide the design, development, deployment, operation, and retirement of services delivered by a service provider with a view to offering a consistent service experience to a specific user community in a specific business context. An SDF is the context in which a service provider's capabilities are arranged into services [10].
- **Service delivery platform (SDP)**– A physical implementation of a service delivery framework.

- **Service oriented architecture (SOA)–** A methodology used to manage the business processes when designing and operating a service delivery platform.

The motivation for developing an SDF is to ensure that a network operators can quickly and easily bring new services and applications to their end-users. Typical wireless network architectures are very complex and successfully delivering services requires interaction with a large number of network elements. Prior to the introduction of SDFs, even very small operators with as few as 100,000 customers delivered services though interaction with billing, rating, charging, intelligent networks, provisioning, SMS, content delivery, and device management systems. Each service required changes to each of these services to enable automatic, consistent, and reliable service delivery. Furthermore, different departments within an operator often managed each system. Best practices concerning change management generally required a full implementation effort to include design, architecture, implementation and testing for each system. This process, in any sized operator could take as long as 6 months. If, on the other hand, an operator brought in a third party, the integration became much more complex because the operator had to provide security measures to ensure that the third party was only performing agreed actions on the network. Thus the SDF was defined to reduce integration complexity and provide a trusted environment for third parties. The goals of a SDF as defined by the Telemanagement Forum [11]:

- Achieve flexible service delivery through integration of functions required for service lifecycle management.
- Manage the complete lifecycle in SOA.
- Maintain control of service lifecycle management across all execution environments.
- Freedom to architect SDPs regardless of vendor and supplier choices.

An SDF is created as an abstraction layer between the complex network elements and the operational and business support systems. The layer simplifies the network and provides a secure environment in which the operator and trusted third parties can deliver services to the operator's customers. The SDF provides three major functions: network abstraction, service execution, and a standard interface to application and service providers. Service Delivery Frameworks have evolved to control services no matter how they are delivered. Early implementations were focused on short message and web applications but modern implementations control services on pure IP data, IP multimedia services, messaging, web browsing, VoIP, and basic voice among others.

Typically the SDF will abstract the multimedia messaging service (MMS), short messaging service (SMS), location services, device management, online and offline charging, billing, IP Multimedia Services, Provisioning, Access Control, Identity Management, Customer Relationship Management, QoS, and network management. This abstraction provides an access controlled, monitored, authenticated, and simplified interface to the network elements and services required to deliver and maintain a service. Many of the interfaces to these elements are very complex with a limited workforce that can successfully utilize them. Furthermore, they are within a trusted domain so there are often no access controls available.

The core of the SDF is an SOA that provides a service creation and execution environment, business rules management, content and management and delivery, service level management, and policy enforcement which interact with the network abstraction defined above.

Finally, the SDF provides a set of interfaces towards operator and third parties based on common protocols like SOAP/XML [12] and OneAPI [13], which can be easily interfaced with their internal systems.

The lessons learned by network operators as SDFs have evolved should be taken into consideration by the NPSBN to ensure that service discovery and delivery are simple, effective, and of the required quality to meet the needs of first responders.

The benefits of an SDF to the NPSBN and PSEN are numerous but a few examples are:

- Applications that are not wireless network aware can be interfaced via a set of simplified APIs rather than raw telecommunications interfaces.
- PSENs can publish applications into the SDF and limit their accessibility to only select groups of subscribers.
- Commercial entities can publish applications into the SDF and one-time, usage, time, or subscription based charging can be managed by the NPSBN rather than a separate relationship for each subscriber.
- These charging and service control mechanisms can be used to spur application development much like the “App Store” environment that currently exists for smartphones.
- As the NPSBN migrates towards machine-to-machine communications, the SDF can be used to provision and manage those devices.

Table 45. Service Delivery Framework Requirement

#	Requirement
1	The NSPBN SHOULD provide a network service (SDF) to allow application developers to published and deploy through common interfaces services and applications to the appropriate authenticated users with permission to use those services.

4.2.7 Identity Management

The NPSBN is expected to enable broadband wireless communication for public safety users. To enable secure access to information, the nationwide system must be able to reliably, securely, and in an interoperable manner, identify users of the network in order to assure appropriate information access. This section pre-supposes the existence of digital identities called identity assertions to describe what the public safety user community needs.

Public safety wants to avoid requiring complex user credential management on the part of their end users. This section describes the need for a framework that will be useful for day-to-day operational use

(e.g., CJIS, CAD, etc.) as well as to enable secured access to information for pre-planned and unplanned mutual-aid scenarios across jurisdictions. The need for an identity management system that works across jurisdictions introduces the concept of identity federation. With the expected proliferation of information, it is impractical to expect end users to manage different credentials for all of the applications and services that they will be required to interact with. Therefore a framework that can manage user identities is required to simplify the life of the first responder, simplify management of their credentials on behalf of the user's administrative staff, and simplify application development by standardizing on the mechanics of user identity and user authentication.

To aid in understanding these topics, identity management and identity federation are defined as follows:

- **Identity Management**–the combination of systems and policies that define the lifecycle of establishing, administering, utilizing, and securing digital identity of individuals. Identity management is intended to simplify both administrative tasks in managing users as well as utilizing digital identities by the end users.
- **Federated Identity**–is the means by which digital identity management credentials can be exchanged securely across boundaries between local, tribal, state, and federal agencies.

Because public safety is likely to have many situations where equipment will be shared amongst different users during different shifts or even during different incidents, an authentication framework that extends beyond LTE device authentication is required. This framework must take into consideration that a single user may in fact share a device amongst different users (e.g., shift-by-shift) or utilize more than one LTE device simultaneously (e.g., vehicular modem, handheld, tablet, etc.).

There is precedent for pursuing standards-based identity federation solutions across government agencies. For example, federal justice agencies have been looking to define methods of providing secure access to multiple agency information systems with a single logon. The Global Federated Identity and Privilege Management (GFIPM) initiative, developed by the U.S. Department of Justice's Global Justice Information Sharing Initiative, provides the justice community with a security and information-sharing architecture that is based on an electronic justice credential. The specific intent of GFIPM is to provide a standards-based federated identity solution to securely connect law enforcement and public safety personnel to interagency applications and data over the Internet. The GFIPM initiative, along with other DHS and DOJ initiatives such as National Information Exchange Model (NIEM), strive for greater interoperability and information sharing across administrative boundaries.

Other examples include federal guidelines such as NIST 800-63-1 (Electronic Authentication Guideline) [14], which provide guidance for electronic authentication, including secure deployment of identity assertions in federated identity deployments. NIST 800-63 was the result of the Office of Management and Budget (OMB) tasking NIST with providing technical guidance on Levels of Assurance (LOA) for the authentication of electronic transactions, as defined in memorandum M-04-04 (E-Authentication Guidance for Federal Agencies) [15]. M-04-04 is part of a foundation of policies that make up the

General Services Administration's (GSA) Federal, Credential, Identity and Access Management (FICAM) initiative.

This subsection describes the requirements of a identity framework as a network service used by users, administrators, and applications to provide a trusted framework to uniquely identify users on the network. Following are requirements for identity framework network service.

Table 46. Identity Framework Network Service Requirements

#	Requirement
1	The identity management framework SHALL enable applications and services to securely verify the identity of users.
2	The identity management framework SHALL be standards based.
3	Identity assertions SHALL be cryptographically protected when being transmitted from one entity to another in the network.
4	The identity management framework SHALL issue identities to non-person entities on the network.
5	The identity management framework SHALL enable non-person entities to authenticate to applications and services where authorized.
6	The NPSBN SHALL define the process and procedures necessary for organizations (local, tribal, state, and federal) to gain approval to join the trust framework.

4.2.7.1 Identity Management Framework

To successfully deploy an identity management system, a framework must be established that can be utilized and trusted by all participating agencies to securely identify users of the system. The establishment of such a digital identity management framework must establish the methods by which user identities are created, issued, used and terminated. This section describes a series of requirements to enable this framework. Wherever possible, this section places responsibility for the management of the individual user on the organization to which the user is affiliated. This is intended to emphasize the local control that public safety has expressed is essential to their day-to-day operational needs as documented in the NPSTC report, "Local Control in the Nationwide Public Safety Broadband Network" [16].

Different organizations (local, tribal, state, and federal) have different requirements for the governance model of the digital identities they will utilize for their organizations. For example, some organizations may vet user identities through FBI background checks and security clearances, while others for example may simply use a state drivers license as proof of user identity when generating a digital identity. The NPSBN identity management framework is challenged with allowing users from any participating agency to be able to identify users from other agencies. Identifying the user and authorizing access to information remains the responsibility of the agency controlling the information.

The NPSBN is responsible for establishing the policies and procedures for which organizations to follow to participate in the identity management framework and ensuring compliance to those policies and procedures on an ongoing basis. Once policies have been established and verified, organizations can join the identity management framework so that the digital identities of their users can be federated and trusted to other organizations within the NPSBN.

To enable interoperable use of the identity information available from the identity framework, a set of attributes and their corresponding format and allowed values must be agreed upon by the public safety community. For example, attributes that describe a user's name, organization or agency, and email address are fairly straightforward. Attributes that describe a user's role (e.g., chief, incident command, patrol officer, utility electrician, etc.) and a user's accreditations (e.g., EMS, paramedic, incident commander, SWAT team sharp shooter, etc.) will require common attribute value definition to ensure that consumers of the identity information can interpret the identity information in a common way. Following are requirements for identity management framework requirements.

Table 47. Identity Management Framework Requirements

#	Requirement
1	Governance of individual digital user identities SHALL be maintained by the local, tribal, state, or federal organization from which the user is affiliated.
2	FirstNet SHALL require that local, tribal, state, or federal organizations establish policies and procedures to govern the digital user identities of users within their respective organizations.

4.2.8 Device Identity Management

The public safety community has some unique expectations for devices that are part of the NPSBN. Public safety has clearly stated that they expect that some devices must be capable of being shared or pooled so that different users, perhaps on a shift-by-shift basis or on an incident-by-incident basis, can use them. At the same time, public safety has stated that they want applications and services to be enabled based on the identity of the human user of the device, not simply on the device itself.

Following are requirements for device identity management**.**

Table 48. Device Identity Management Requirements

#	Requirement
1	NPSBN devices SHOULD be capable of being shared amongst different authorized human users.

4.2.9 Authentication Services

This section describes requirements for authentication within the NPSBN. Authentication is a critical function of the network and as such has implications on trust, governance, and network monitoring.

Table 49. Authentication Services Requirements

#	Requirement
1	A NPSBN governance framework SHALL be established that identifies a set of security policies for agencies to participate in the identity management framework and to remain included in the framework over time.
2	The NPSBN SHALL have access to the identity management framework for purposes of user activity monitoring, security monitoring, and application delivery.
3	The NPSBN identity management framework SHALL enable both NPSBN- and PSE-based applications and services to verify the identities of users irrespective of authorized administrator (both FirstNet and PSEN) management of the user's authentication credentials.
4	The NPSBN authentication services SHALL support industry standard authentication interfaces for mobile and fixed infrastructure components.

4.2.10 Authorization Services

Once a user has been authenticated via the identity management framework, the user will attempt to utilize their identity information to access information within their home network, the network of another jurisdiction, and regionally. Following are requirements for authorization services.

Table 50. Authorization Services Requirements

#	Requirement
1	The identity management framework SHALL manage privileges for person and non-person entities.
2	Services and applications SHALL authorize access to information based on the identity of users, their roles, and other attributes based on policies for the services and applications.

4.2.11 Device Management

The NPSBN must provide a network service that allows an authorized entity to perform a wide array of device management functions on the UEs on the network. The functions provided by the device management network service affect the UE through its lifetime on the network and range from the initial configuration of the UE, through ongoing maintenance and monitoring of the UE, to the final deactivation of the UE. Device management network services are only available to authorized entities, which may include administrators, applications, and applications users. UEs may be associated with a user, or may not be associated with a user, such as an authorized, remote video camera.

All device management functions described in this section refer to on-network operations.

4.2.11.1 Initial Configuration

In order to access the NPSBN, users will need to have access to UEs that are capable of attaching to the NPSBN and supporting the user needs. It is envisioned that a jurisdiction may have a quantity of UEs ready to activate at some point in the future, or the jurisdiction may have a UE that was ordered specifically for a particular application and/or user. The process local jurisdictions use to receive, activate, and configure UEs should be as simple as possible, while retaining security on the NPSBN.

To enable new UEs to access the NPSBN, the SIM associated with the UE needs to be programmed with a minimal set of information, such as the PLMN ID of the NPSBN. As long as this minimal set of information is provided in the UE and the HSS is provisioned with the UE-associated information, there are widely accepted mechanism based on OMA-DM standards that will configure the UE with the specific information for that UE, such as specific APN information, etc. This does not require the UE user to do any programming. Following are requirements for initial UE configuration.

Table 51. Initial UE Configuration Requirements

#	Requirement
1	The NPSBN SHALL provide a user portal that allows a jurisdiction to configure new UEs with their specific information.

4.2.11.2 Configuration

Users must be able to access one or more PSENs while using their UEs. In some cases, users will only access a single PSEN at a time, such as when a user occasionally supports the neighboring jurisdiction. In other cases, users may need to access more than one PSEN at the same time, such as a state police officer which may need to interface with the local jurisdiction and the “home” PSEN. The device management network service must allow an authorized entity to configure the PSENs a user or UE is capable of accessing. Similarly, the UE must be able to be configured to access various wireless networks such as Wi-Fi or commercial cellular networks. As the user of a UE changes, the PSEN addresses and wireless network information the user is able to access must be available.

Users may be involved in critical situations in which modifications to their equipment may be undesirable. These may be short-term events such as a SWAT team responding to an incident, or a longer term event such as public safety officers providing support of Mardi Gras. In these scenarios, it would be useful to lock down the configuration of the affected UEs to prevent changes to their operation during these critical scenarios. Following are requirements for device management configuration.

Table 52. Device Management Configuration Requirements

#	Requirement
1	The device management network service SHALL allow an authorized entity to configure application clients on a UE to be able to access one or more application servers in PSENs.

#	Requirement
2	The device management network service SHALL allow an authorized entity to configure application clients on a UE to be able to access one or more PSENs based on the user of the UE.
3	The device management network service SHALL allow an authorized entity to configure a UE to be able to access one or more wireless networks.
4	The NPSBN SHALL support Over-the-Air (OTA) SIM management.
5	The NPSBN SHALL support OTA Firmware Update management.
6	The NPSBN SHALL support OTA Software Configuration management.
7	The NPSBN SHALL support OTA APN connection management.
8	The NPSBN SHALL support OTA Diagnostics Monitor (e.g., LTE radio statistics) management.

4.3 Transport Services

This section is intended to describe the overall connectivity requirements of the NPSBN. The network consists of much more than just an LTE network. The scope includes all end-to-end connections provided in this network.

This section will not describe the specific transport technologies (i.e., fiber, microwave, MAN), but define the connections allowed by the network, the paths through the network to the various services provided to the users. It will also define any optional features that will be required by the overall network.

4.3.1 Supported Transport Paths

The NPSBN architecture must provide transport paths to/from all devices, entities, and networks. Following are transport path requirements for the NPSBN.

Table 53. Transport Path Requirements

#	Requirement
1	The NPSBN architecture SHALL provide transport between a NPSBN-U and its home PSEN.
2	The NPSBN architecture SHALL provide transport between a NPSBN-U and non-home PSEN as needed.
3	The NPSBN architecture SHALL provide transport between a NPSBN-U and the PSTN. (This is required if PSTN service is implemented at launch.)
4	The NPSBN architecture SHALL provide transport between a NPSBN-U and NPSBN Services.

#	Requirement
5	The NPSBN architecture SHALL provide transport between a NPSBN-U and NPSBN O&M Services.
6	The NPSBN architecture SHALL provide transport between a NPSBN-U and 9-1-1call centers.
7	The NPSBN architecture SHALL provide transport between a NPSBN-U and another NPSBN-U attached to the same EPC.
8	The NPSBN architecture SHALL provide transport between a NPSBN-U and another NPSBN-U attached to a different EPC.
9	The NPSBN architecture SHALL provide transport between a NPSBN-U and a commercial roaming exchange.
10	The NPSBN architecture SHALL provide transport between CMAS and a NPSBN-U.
11	The NPSBN architecture SHALL provide transport between NPSBN Services and a PSEN.
12	The NPSBN architecture SHALL provide transport between NPSBN Services and NPSBN O&M Services.
13	The NPSBN architecture SHALL provide transport between NPSBN Services and 9-1-1call centers.
14	The NPSBN architecture SHALL provide transport between NPSBN Services and the PSTN. (This is required if PSTN service is implemented at launch.)
15	The NPSBN architecture SHALL provide transport between NPSBN O&M Services and a PSEN.
16	The NPSBN architecture SHALL provide transport between a PSEN and commercial networks.
17	The NPSBN architecture SHALL provide transport between a PSEN and a NPSBN EPC.
18	The NPSBN architecture SHALL provide transport between NPSBN O&M Services and a NPSBN EPC.

4.3.2 Nationwide Private IP Network

The NPSBN must provide connectivity between itself and all IP networks that interface with it. This IP network, created and controlled by FirstNet, will provide IP connectivity; for example, from an agency's PSEN to the NPSBN's EPC that is geographically closest to that agency. Similarly, that same IP network will connect the NPSBN Services to the EPC that is geographically closest to it. This IP network is the "connectivity tissue" that allows all of the geographically separated enterprise networks connection into the NPSBN LTE network.

It is assumed that the private IP network will be required to provide all of these interfaces. The term "private IP network" here means that FirstNet has control over the network and can specify its performance characteristics. The fact that portions of the network may be VPNs is not a problem. This means the physical equipment may be shared with other public or private entities, but the performance and addressing of the network is fully within the control of FirstNet. There is no constraint intended to limit the IP addressing to RFC 1918 [24] private IP addressing restrictions.

The physical makeup of the nationwide private IP network is not defined here. There is no assumption made here that assumes one ubiquitous physical IP network. This could be made of various different IP networks and physical connections from different network providers as long as it meets the requirements and provides a VPN over public networks.

There is no requirement here to force different connection points, or PSENs, or anything else to be transported on separate physical or logical networks. The intent of this section is to define a private connectivity network that transports packets from various, separate networks into the NPSBN IP network.

This section attempts to define the generic requirements that this connecting private IP network must provide. There is no intent to define requirements for the connected PSEN networks, for example. These requirements only apply to the network that connects them all to the NPSBN. Subsequent sections of this document define specific requirements that exist for specific interfaces.

4.3.2.1 General Requirements

It is assumed that the nationwide private IP network must provide the performance required to allow mission-critical data applications to operate during incidents and disasters and must maintain a minimum level of service and reliability during such incidents. Following are general requirements for the nationwide private IP network in the NPSBN.

Table 54. General Requirements for the Nationwide Private IP Network

#	Requirement
1	The nationwide private IP network SHALL support route diversity to provide public-safety grade reliability.
2	The nationwide private IP network SHALL support end-to-end QOS. This is to guarantee a defined QOS behavior from an application to the UE.
3	The nationwide private IP network SHALL support power backup for public safety-grade level of continuous electricity outage.

4.3.2.2 PSEN Connectivity

Some local agencies may not desire their PSEN to be connected directly to the nationwide private IP network. This may be because they don't want to pay for additional backhaul to connect to the NPSBN IP network or because there is no physical way to do it due to the rural location of the agency.

During mutual aid scenarios, any user may desire to change the agency they are connected to, or even to be connected to multiple agencies at the same time.

Following are requirements for PSEN connectivity in the NPSBN.

Table 55. PSEN Connectivity Requirements

#	Requirement
1	The NPSBN SHALL allow a user (NPSBN-U) to define which agency(s) PSEN it desires to connect to and provide dynamic connectivity to that agency's IP network (PSEN).
2	Agencies' PSEN SHALL be allowed to connect to the NPSBN through the Internet and not be required to support a physical connection.

4.3.2.3 Local PSEN Interfaces

Different local agencies have different types of networks. The nationwide private IP network must provide flexibility to allow interconnection with these different types of IP networks. Following are requirements for PSEN connectivity in the NPSBN.

Table 56. PSEN Interoperability Requirements

#	Requirement
1	The nationwide private IP network SHALL connect to PSEN networks that support Internet Protocol version 4 (IPv4), and other PSEN networks that support Internet Protocol version 6 (IPv6).
2	The nationwide private IP network SHALL allow legacy IP applications to work through the network to the NPSBN-U. (NAT may cause some existing applications to fail. Some examples of these applications are any applications using SIP or SNMP)
3	The nationwide private IP network SHALL provide enough bandwidth to support the capacity necessary for the user's applications that are connected.

4.3.3 Access to Local Applications and Services

Agencies have already made a large investment in applications hosted locally that are used every day in their workflow. Many agencies can already access these applications using commercial networks. There is a requirement for the NPSBN to enable access to these applications.

A PSEN can serve an entire state, depending on the agencies (PSEs) involved, or a single agency. PSE networks are private and secured. There is a desire to authenticate users with the PSEN before allowing the user's device access to the PSEN. To establish connectivity between the NPSBN and a PSEN, a transport network will be required. The planning and cost of such a connection is out of scope for this high-level launch Statement of Requirements (SoR). In general, the connection is expected to be private.

Use of a secure connection via the Internet is also possible but will limit the ability to use QoS functions. The NPSBN should support either model to meet the needs of all agencies.

Agencies that use commercial services secure the communications using an over-the-top VPN or mobile VPN (MVPN). Securing the connection is typically done for access to restricted databases. Some agencies have contracted with the commercial network provider for private connections between the commercial network and the PSEN. These connections have better performance and some additional security but also additional cost. Since the commercial service may serve as a backup service to the NPSBN LTE service, the use of VPN or MVPN service will continue for some agencies.

The expectation is that only members of the agency will be connected to the associated PSEN under most circumstances. As the network evolves and identity management of users is better defined, the network should support connection of members of different agencies to critical local applications. Several methods including access to the PSEN by non-agency users when in a mutual aid scenario should be considered.

Not all agencies may require local connectivity (own a PSEN).Some agencies may choose to use national applications and Internet access only. Following are requirements for access to local applications and services in the NPSBN.

Table 57. Requirements for Access to Local Applications and Services

#	Requirement
1	The NPSBN SHALL support an agency's ability to perform a secondary authentication before allowing an NPSBN-U to connect with a PSEN.[2]
2	The NPSBN SHALL support a communication path between an agency's NPSBN-U's and the PSEN without imposing a NAT.[3]
3	The NPSBN SHALL support local IP applications in the PSEN.[4]
4	The NPSBN SHALL support transport of VPN traffic from an NPSBN-U to the PSEN.[5]
5	The NPSBN SHALL support transport of prioritized traffic from/to the PSEN.

[2]A secondary authentication should be at agencies' discretion. The secondary authentication will require modifications to the devices and PSEN equipment to perform the secondary authentication. The secondary authentication is for access to the PSEN and may or may not be coordinated with a unified identification used for NPSBN services.
[3]If required by an agency, the NPSBN should utilize PSEN address space for NBN-U's connecting to that PSEN. This requirement is to minimize impact on the existing PSEN equipment and applications in private address space which may not function through a NAT. There may be additional reasons for a NAT to be introduced in the device or in the agency that are out of the scope of this requirement. An agency could additionally choose connectivity via a NAT if the agency already has NAT friendly applications.
[4]There is no guarantee that all applications will work over the NPSBN. Minimally applications that already work on commercial will work on the NPSBN. Not all agencies will require connectivity to a PSEN.
[5]This allows existing VPN or mobile VPN equipment to be used. Not all agencies use VPNs or MVPNs.

4.3.4 Access to NPSBN Services

This section addresses transport requirements to support authorized user access to NPSBN services. An authorized user as it relates to the below requirements is the device user, not the device itself. It is envisioned that in many cases, the device will be hard-mounted and inaccessible to the user. As such, any user identity associated with the SIM in the device may not be applicable to the actual user of the device. Further, this section is not intended to articulate any proposed way to authorize the user. It is expected that the user be properly authorized as defined by FirstNet.

Authorized users may attach to the NPSBN services over a NPSBN LTE connection, a commercial network, a wired or wireless connection from a PSEN, or any other network that is attached to the Internet to access said services. Some services will take specific network paths based upon their applicability such as Short Message System (SMS) messages, which would not typically traverse a PSEN wireline network for user access. Further, many of the connections will be through a Mobile Virtual Private Network (MVPN) connection to allow both virtual Point-to-Point access to the user's PSEN and the passing of sensitive or privileged information.

Note that while most transport requirements assume access to services would be from a PSEN, it is not technically reasonable for certain NPSBN services (i.e., PSTN, SMS, MMS, etc.) to traverse this defined path. These types of services will be provided directly to the NPSBN-U connected to either the NPSBN or when in a roaming state on other networks. When reviewing these requirements, this fundamental concept is assumed. Requirement #1 and #2 in Table 58address access to these services directly by the NPSBN-U. Finally, based upon that path, note that it might not be possible to apply QoS, e.g., NPSBN user roaming onto a commercial 3G network. As such, application performance expectations should be adjusted accordingly.

This section does not address any security concerns associated with the various access requirements. Requirements for secure access to NPSBN services are addressed in Section 5.18 as those requirements relate to network transport. Following are transport requirements for access to NPSBN services.

Table 58. Requirements for Access to NPSBN Services

#	Requirement
1	NPSBN services SHALL be accessible directly from a NPSBN-U connected to the NPSBN by an authorized user.
2	NPSBN services SHALL be accessible directly from a NPSBN-U connected to a commercial or other network by an authorized user.
3	FirstNet SHALL size the connections to each PSEN in accordance with the SLA with the PSEN.
4	NPSBN services SHALL be accessible by authorized users, over a FirstNet provisioned MVPN, if provided, originating on a NPSBN-U, and terminating on the NPSBN.

#	Requirement
5	NPSBN services SHALL be accessible by authorized users over a FirstNet provisioned MVPN, if provided, originating on a NPSBN-U roaming to a commercial or other network, and terminating on the NPSBN.
6	NPBSN services SHALL be accessible from a PSEN by authorized users connected to the PSEN via any means.
7	NPSBN services SHALL be accessible from a PSEN by authorized users connected to the PSEN by any means via an encrypted link provisioned from the PSEN to the NPSBN services.

4.3.5 Mobility

This section provides public safety requirements on NPSBN capabilities for supporting user mobility. The following definitions apply for the purposes of the requirements in this section.

Mobility management is a key element of the NPSBN that allows user equipment to work across the network. The aim of mobility management is to track where the user equipment (UE) is allowing services to be delivered to the UE.

Handover is the process of maintaining active session(s) as the UE moves, traversing parts of the network's coverage area that are served by different cells. Handover allows sessions associated with UE to be transferred from one cell site to another cell site in the wireless network. To provide a seamless handover experience, the length of time that it takes for the UE to switch between the two cell sites (called the interruption time) must be minimized.

Roaming is the process supporting the movement of UE outside the geographical coverage area of its home network. Roaming allows the UE to automatically send and receive data when within the coverage of a network with a different PLMN identity than the UE's home network. This network with a different PLMN identity is called the visited network. Roaming is also subject to UE capabilities, as the UE must support the radio access technology and the spectrum band of the visited networks in addition to the home network. The roaming process does not preserve user data sessions; they have to be re-established in the visited network after successfully completing the roaming process. Roaming is addressed herein only in the context of roaming between the NPSBN and commercial cellular networks.

Support of session persistence when users roam to other networks can be provided using add-on solutions, e.g., an MVPN solution or a broadband bonding solution.[6] The user may experience a short interruption depending on the specific solution selected. MVPN solutions are currently in use by public safety to, for example, support service continuity between commercial wireless networks and Wi-Fi. In the NPSBN, individual agencies can decide whether to use MVPNs or other add-on solutions, and which vendor equipment to use.

[6] A broadband bonding solution aggregates multiple connections to achieve a faster, more reliable service. Bonding solutions could be used to provide continuous service for demanding applications such as high quality video on the move.

When used for guaranteed bit rate services with dedicated LTE bearers, an MVPN will be able to maintain service availability, but the visited network may not be able to provide the same quality of experience. For example, if a user is sending real-time video on LTE and loses LTE connectivity, the new network may not have the bandwidth available to continue this video service with the same quality of experience.

Following are mobility requirements for NPSBN-U equipment on the NPSBN.

Table 59.Mobility Requirements

#	Requirement
1	The NPSBN and NPSBN-U equipment SHALL support NPSBN-U mobility across the entire NPSBN.
2	The NPSBN and NPSBN-U equipment SHALL support NPSBN-U roaming from the NPSBN to commercial networks as per established roaming agreements.
3	The NPSBN-U equipment SHALL automatically roam back to NPSBN when a NPSBN-U returns to adequate coverage of NPSBN regardless of the coverage situation of the visited network and when the UE is idle. Note: Care must be taken with algorithms in the device to avoid ping-ponging between networks along borders of the NPSBN, which will provide a poor user experience and utilize excessive network resources.
4	The NPSBN SHALL support the PSEN use of solutions; for example MVPN technology that provides session persistence when a NPSBN-U is roaming from the NPSBN to commercial networks as per established roaming agreements.

4.3.6 Public Internet Access

Access to the Internet from UEs is a vital valuable service the NPSBN can provide to users. That access must be provided with strong security measures to protect the NPSBN from harm and security breaches. Some agencies prefer that their user's access to the Internet be via the agency's own PSEN. Some users require VPN transport service via the Internet. For example, in some cases users will need access to secure data that is not hosted by the PSEN and only available using the Internet. VPN service will allow secure access to that data not available via the PSEN. In addition, some agencies policies will require the need for them to deny Internet access to their own users. Following are public Internet requirements for UEs on the NPSBN.

Table 60. Public Internet Requirements

#	Requirement
1	NPSBN-U SHALL have access to the Internet via NPSBN transport to access any Internet provided service or data.

#	Requirement
2	The NPSBN SHALL allow VPN access to data via the Internet transport.
3	The NPSBN SHALL be protected against attack via the Internet access and PSEN's shall follow FirstNet security policies.
4	User agencies SHALL have the option to block Internet access to their user devices.
5	User agencies SHALL have the option to provide Internet access to their devices via their own agency Internet transport.

4.4 System Design

The contractual agreements between PSEs, or states, and FirstNet will likely include guaranteed service levels in terms of radio coverage, system performance, and network availability within a defined operating area. This section defines a minimal set of associated requirements as a basis for the design of the NPSBN. They reflect what the community of public safety end-users is expecting from FirstNet and the NPSBN.

As is generally the case in wireless deployments, the applicable design requirements will translate into measurable key performance indicators (KPI) which will form the basis for acceptance testing activities and network optimization, prior to service launch but also for post-launch reporting and monitoring. Neither the design validation methodology, nor performance assurance, is addressed herein; there is an expectation for extensive testing performed by respondents to the RFP. Finally, since system design requirements drive the overall cost and phased deployment of the system in terms of equipment, services, and operational costs, there is an expectation for a balanced design approach particularly with regard to the users' service charges that result.

4.4.1 NPSBN Considerations for Traffic Models

It is common industry practice to refer to specific traffic models in order to highlight performance objectives. This section is informative and provides consideration for traffic models that may form the basis for the performance requirements; a few key traffic model attributes are provided for reference purposes only.

Public safety use of the NPSBN will vary dramatically across the country. For example, in one area, the use of mobile streaming video may be extensive. Whereas in another area, high-definition image use may be more typical. As another example, one agency may equip every firefighter with biometrics and streaming video capability, while another agency may not have sufficient resources to outfit their departments with such technologies. Further, the expectation is that the NPSBN will satisfy both day-to-day users and multi-agency incident users demand within limits of the available capacity.

There are multiple ways of defining traffic models for the purpose of designing the NPSBN but, ultimately, applications will map to certain traffic demand per category of users. In addition to defining

performance objectives the purpose of using traffic models is to properly account for spatial traffic demand when designing the RAN, including coverage, as well as sizing the backhaul network, gateways, and other network and core components. Traffic considerations for a particular region might include the following attributes:

- (Static) Spatial geographic densities as a baseline for the design.
- One or more traffic profiles per user or device category depending of the operational environment.
- Proportion of active users, i.e., representing the number of concurrent users in the system, which is a function of operating shifts.
- Day-to-day traffic loads and busy-hour contribution. Since incidents can occur anywhere, traffic density can effectively shift across the region. Therefore, the number of concurrent users per coverage sector or cluster of cells might be useful or the selection of a scaling factor would be sufficient.
- Application characteristics such as real-time/non real-time services, uplink/downlink data rates, average message (packet) size, bearer activation rate, and percent mix of each application.
- User/device characteristics including the attach/detach rate, idle to active transition frequency, and the accessibility and retainability priority setting of each user/device.[7]
- Mobility characteristics, including mobility within the NPSBN and mobility to the commercial network. The important parameters include the percentage of roaming users/device, intra- and inter-network handover frequency, application/user/device accessibility, and retainability during roaming.

Further, there may be expectation for data growth over time because of change in user behavior or change in the population size. Given these parameters in conjunction with other system design data, one can correctly size a system for local, tribal, state, or federal needs. Initial traffic models should take that growth into account so that the network can handle the volumes, at least until a substantial network evolution is planned. Specific models for various public safety activities will be provided in a later phase of the SoR development.

4.4.2 Performance

The ability for the NPSBN to transport public safety applications with the required quality, and when needed, within the NPSBN service area, will be a function of the performance requirements imposed on the network. Devices and applications, including servers, sources, and clients, can impact performance but these are not covered herein. The ability of the system to efficiently share available resources, to carry and maintain sessions, to provide access anytime and anywhere within the designated service area, while mobile or fixed, are examples of performance-related factors.

[7] Accessibility: The ability to access services. Retainability: The ability to maintain an ongoing session.

Latency, average and minimum user throughput, percentage of successful connections, percentage of successful intra-NPSBN handovers, or percentage of dropped sessions are examples of grade of service (GoS) metrics which could be used for design, or service level, acceptance. Further, since the legislation [1] addresses the possibility of leasing scenarios, appropriate safeguards such as priority shall be required when sharing resources with secondary users. Ultimately, because of their primary use of the system, public safety users expect a better service performance to be offered by the NPSBN than by a commercial network.

The public safety GoS metrics identified in Table 61 could be directly translated into, and, in some cases identical to, KPI, Is expected to be reported by FirstNet in contractual agreements. Because of traffic growth or network expansion, e.g., RAN expansion, and upgrade, a network design is never completed but is optimized on a regular basis for improvement in service levels hence in users experience. Therefore, while performance metrics may not change, performance targets may. These will be addressed in a future version of the SoR. Further, performance bottlenecks can occur anywhere from applications servers to the UE; our focus herein is on the NPSBN infrastructure.

Following are performance requirements for the NPSBN.

Table 61. Performance Requirements

#	Requirement
1	The NPSBN SHALL guarantee a level of accessibility and retainability of critical services across FirstNet's service area throughout the different deployment phases.
2	The NPSBN SHALL be designed according to measurable GoS levels throughout the NPSBN service area.
3	The NPSBN SHALL be designed so that applications transported through the NPSBN meet a minimum performance criteria identified by applicable Quality of Service (QoS) standard specifications (e.g., in terms of delay budget and packet loss per QCI).
4	The required data throughput performance of applications SHALL be maintained at vehicular speeds.
5	The use of the NPSBN by secondary users, i.e., non-public safety services, SHALL NOT affect the performance experienced by primary public safety users.
6	To mitigate performance-impacting interference issues for current and planned deployments at international borders, the design of the NPSBN SHALL account for any known spectrum usage and bandplans of the neighboring countries.
7	To ensure a reasonable end-to-end quality of service, performance level benchmarks SHOULD be included in roaming agreements between FirstNet and commercial carriers.
8	The NPSBN SHALL be engineered to prevent traffic congestion at every stage of the network to meet the NPSBN GoS objectives.

#	Requirement
9	The NPSBN SHALL support capacity and/or coverage expansion to address evolving users needs.
10	The design of the NPSBN SHALL account for higher traffic demand in areas deemed strategic by FirstNet and/or PSEs.
11	Intra-NPSBN handover SHALL NOT be perceptible to the user.
12	The use of standard-compliant high-power NPSBN UEs SHALL NOT create harmful interference to any UEs' NPSBN services.
13	Transmission from a NPSBN UE SHALL NOT affect the receive performance of its GPS receiver (if embedded) or other GPS units in close proximity (e.g., navigational devices).
14	NPSBN radio equipment, including UEs, SHALL comply with applicable standards specifications and regulatory mandates.

4.4.3 Coverage

Coverage is generally associated with an expected data rate or service, therefore, a particular service area should map to one or more specific levels of service each identified by a coverage reliability and a minimum guaranteed service. FirstNet is expected to work with PSEs to define a coverage GoS level for each identified service area. For example, per operational needs, some jurisdictions may require a minimum of on-street portable coverage across all morphologies for a video service while others require indoor coverage in urban areas for voice services. Also, because of terrain ruggedness, sparsely populated areas, or lack of antenna structures, coverage reliability may be lower than in urban areas.

Although the legislation refers to ensuring substantial rural coverage, the phased deployment of the NPSBN may call for coverage to be complemented by means of deployable assets (during major incidents), roaming or partnership with commercial carriers.[8] FirstNet is likely to leverage existing PSE's assets but depending on the targeted sites density, the potential lack of a sufficient number of suitable sites or antenna structures would lead FirstNet to either reinforce existing public safety assets, develop new ones, or rely on third-party partners such as tower providers to build the network. On the other hand, poor coverage in environments such as underground facilities is expected to be improved at some point via the use of small cells, repeaters, distributed systems, etc.[9]

The desire to transport services to/from airborne UEs was expressed a number of times by the public safety community in view of the clear (operational and situational awareness) benefits of such a service. However, because aircrafts' altitude, speed, and random flying patterns can lead to serious interference issues with ground systems, it is common (regulatory) practice to assign dedicated channels as exemplified by narrowband and/or broadband spectrum allocations in both the public safety and

[8] Details of such public private partnership arrangements are yet to be determined.
[9] Coverage of indoor facilities shall meet National Fire Protection Association – NFPA 72, 2013 edition, Chapter 24, (24.5.2).

consumer markets. Further, although air-to-ground operation may be considered (by the FCC) on a secondary basis to land-based NPSBN operations [17], it is understood that more work is needed to assess its feasibility. Therefore, the topic is not addressed herein.

Following are coverage requirements for the NPSBN.

Table 62. Coverage Requirements

#	Requirement
1	FirstNet SHALL provide coverage in the service area(s) required by PSE.
2	The service area SHALL include, but not be limited to, all or any of the following if applicable: population clusters, critical buildings or light/commercial facilities, transportation infrastructure (highways, primary roads, bridges, etc.), critical infrastructure, strategic international border crossings, and coastal areas.[10]
3	The coverage GoS level(s) attribute SHALL include but not be limited to: minimum data rates, percentage of coverage and coverage reliability for each applicable environment (urban/non-urban, indoor/outdoor, portable/vehicular) and region(s) specific to the PSE.
4	FirstNet SHALL coordinate with PSEs and commercial cellular providers, and towers/buildings providers, for the antennas placement and equipment location to minimize inter-system interference issues.
5	Coverage validation SHALL follow industry “best” practices.
6	The RF planning and design of the NPSBN SHALL account for the possible coexistence of standard-compliant low and high-power UEs.

4.4.4 Reliability

This section describes requirements pertaining to the reliability of the NPSBN infrastructure supporting NPSBN services. Reliability aspects of user devices are covered in the UE section. There is an expectation for the NPSBN infrastructure to be highly reliable or at least more robust than commercial providers’ infrastructure with a targeted network availability better than, or on par with, existing land mobile radio systems. For example, commercial wireless providers are already required by the FCC to provide emergency backup against loss of commercial power with some exceptions, e.g., on the basis of applicable local laws [18].

Table 63. Reliability Requirements

#	Requirement
1	The NPSBN infrastructure's availability SHALL be typical of a public-safety grade network.
2	Issues impacting availability SHALL be managed within agreed SLAs.

[10] Perhaps, tunnels and other underground environments could be phased over time.

The intent of this section is not to dictate a particular architecture for the NPSBN, or a certain level of redundancy for each network element, but to ensure the network is designed such that service-impacting components or link failures are kept to a minimum. This should not be confused with the usual coverage reliability metric, e.g., 95-percent location variability, used in network designs to indicate the level of confidence in the service area. In that regard, because of the distinct applications that may be carried over this wireless multimedia network, distinct service-level availability figures will apply since the reliability paths can differ. The focus herein is on infrastructure and not on whether, for example, a voice service should be more reliable, less reliable, or as reliable than a video service. The goal is for a reliable service or services across the whole NPSBN service area.

As noted above, the NPSBN infrastructure should be designed for high reliability; however, a failed radio site may happen. Since the public safety LTE network is expected to operate with a frequency reuse of one (i.e., a single channel), it is not practical to have complete overlapping cell coverage (overlapping areas have significant co-channel interference - reducing throughput) as typical of PSEN radio networks. In the event of a loss of coverage due to a failed radio site, an adjacent site from the NPSBN may be able to provide partial coverage but the user experience may be reduced and not all services may be available in that 'outage' area. For example, a user may be able to re-attach to the network and run a voice service, but the ability to execute a video service will be diminished because of the lower throughput experienced. Other alternatives may be to build a denser network to leave sufficient margin for (automated or manual) antenna adjustment or hand-over to a commercial cellular network if such a service is available. Further, ongoing activities in the 3GPP standardization body on heterogeneous networks, interference coordination, and interference rejection should help to provide improvements in the long term.

4.4.5 Resiliency

This section contains requirements on the ability to recover from localized disasters (e.g., a hurricane) by deploying temporary assets to provide interim communications and similar requirements.

Since redundancy, hardening, sheltering, etc. applied across all regions or sites and facilities will be expensive and could lead to delays in initial service launch or reduced coverage a balance must be struck between what is necessary and what is desired. Lessons learned from past disasters taught us that telecommunications should be better built whenever possible and that workable contingency plans should be in place to allow for service continuity. FirstNet has the option of complementing the land-based wireless infrastructure for which it has a spectrum license with other means such as airborne or satellite platforms. Provisioning of satellite services via a third-party entity is a separate business arrangement. While the table below makes reference to 'outage' we have yet to define it.

Following are resiliency requirements for the NPSBN.

Table 64. Resiliency Requirements

#	Requirement
1	Deployable access nodes or systems, e.g., cell-on-wheels, system-on-wheels, or airborne systems, SHALL be made available to the states for (rapid) deployment to deliver capacity or coverage when needed.[11]
2	Service restoration time following an outage SHALL be minimal as per a service level agreement.
3	Scheduled maintenance SHALL have minimal impact on services.
4	Silent failure modes, i.e., failed backup components that have gone undetected, SHALL be minimized.
5	The network SHALL revert to its original state of operation upon failure resolution.
6	Adequate spare parts, antennas, transmission lines SHALL be stocked by the servicing agency.
7	Remote reset of RAN equipment SHALL be available at each site.
8	Any redundant NPSBN core SHALL support the full RAN traffic load.[12]
9	Shelters housing NPSBN equipment SHALL be hardened according to best practices employed in the region.
10	The design of the NPSBN SHALL account for the following: Electromagnetic Interference (EMI), lightning protection, power surge protection, and tower wind loading.

4.4.6 Backhaul

This section describes backhaul categories and needs.

Since the legislation is not clear on the backbone segment, i.e., the linkage between regional RAN and FirstNet's core and data centers, the focus herein is on the regional links, i.e., the state or multi-state backhaul component of the NPSBN. Some of the availability text may appear redundant to the Reliability section but these are specific to the backhaul transport. There is no particular distinction between microwave and fiber physical transport.

Following are backhaul requirements for the NPSBN.

[11] Per critical region, e.g., an Urban Area Security Initiative (UASI). Moreover, there is an expectation that backhaul means will be part of the deployable solution.
[12] A single core location could house multiple EPCs

Table 65. Backhaul Requirements

#	Requirement
1	Backhaul links SHALL be designed for high availability.
2	Design of the backhaul SHALL account for traffic overloads, e.g., during large-scale events.
3	Backhaul links SHOULD be engineered to distinguish (or segregate between) PSEN traffic from (and) secondary users traffic when applicable.
4	Backhaul transmission delays SHALL support the end-to-end delay budgets established for latency-sensitive applications.
5	Switchover time from a primary path to a redundant path SHALL be imperceptible to LTE-users.
6	All backhaul and inter-connect sites SHALL be protected against loss of commercial power.
7	Secure remote monitoring, configuration, troubleshooting, and reset of transport equipment SHALL be available at each node.
8	The backhaul network SHALL be scalable to accommodate traffic growth.

4.5 User Equipment

This section describes requirements for User Equipment (UE) that are expected to be utilized by Nationwide Broadband Network Users of the NPSBN. The UE is a device that connects to the NPSBN Radio Access Network (RAN) via the Long Term Evolution (LTE) air interface and provides the wireless connectivity for mobile data and applications services, including voice. For example, at least some public safety users will require emergency button functionality that provides services similar to the emergency buttons in LMR radios.

For future phases, NPSBN-Us will need various levels or “tiers” of ruggedization and security that exceeds that of current consumer UEs. For example, NPSBN-Us will require public-safety grade levels of device intrusion protection, environmental countermeasures (e.g., water resistance), security management, and human-machine interface (also known as HMI) accessibility, etc. There will also be NPSBN-Us who employ standard consumer-grade UE devices that are capable of operation on NPSBN frequencies.

A variety of UE consumer devices such as smartphones, Personal Computers (PCs), tablet PCs, modems, and customer premise equipment (CPE) in fixed, portable, and vehicular configurations are available today for operation on commercial networks. Public safety expects that equivalent devices, capable of operating both on commercial networks and on the NPSBN, will be available.

The following sections identify the basic device types and specific public safety requirements beyond those normally associated with the given types of devices. Unlike other sections of this document, the

stated requirements are not requirements on FirstNet or the NPSBN per se, but represent public safety's particular device needs. Note that these requirements do not attempt to identify all of the software defined features of UE (such as, telephony support or PTT functionality), but focuses instead on the characteristics of the UE itself.

4.5.1 UE Device Types, Operating Environments, and Features

Following are requirements for UE device types.

Table 66. UE Device Types Requirements

#	Requirement
1	NPSBN-Us SHOULD have consumer-equivalent smartphones capable of operating on both commercial networks and the NPSBN.
2	NPSBN-Us SHOULD have consumer-equivalent tablet PCs capable of operating on both commercial networks and the NPSBN.
3	NPSBN-Us SHOULD have vehicle mount modems capable of operating on both commercial networks and the NPSBN that meet public safety requirements for in-vehicle installation.
4	NPSBN UE devices SHOULD be able to accommodate multiple users and associated user personalities on a single device (i.e., use of a single UE device to support multiple shifts).

4.5.2 UE General Requirements

UE devices need to satisfy the functional requirements of the network as outlined in this document. This section describes the general requirements for a UE that will be employed by public safety users of the NPSBN. These requirements apply to any NPSBN capable, commercial service-capable, or other wireless service (i.e., leased spectrum authorized by FirstNet) device employed by NPSBN-Us.

Following are general requirements for UE devices.

Table 67. UE General Requirements

#	Requirement
1	NPSBN UE device SHALL provide a clear indication to the NPSBN-U when the UE device is roaming (not using the NPSBN).
2	NPSBN UE SHALL support dual stack IPv4/IPv6.
3	NPSBN UE SHOULD support enhanced autonomous location services (e.g., latitude, longitude).
4	NSPBN UE SHOULD operate at power levels to meet the NPSBN coverage needs.

4.5.3 UE Interoperability

There are a significant variety of coders and decoders (CODECs) that convert analog voice and video into digital form for transmission on digital systems. FirstNet will need to select a minimum set of voice and video CODECs that must be resident on all NPSBN UE devices to facilitate interoperability.

Following are interoperability requirements for UE devices.

Table 68. UE Interoperability Requirements

#	Requirement
1	The NPSBN-U SHALL have UEs that support FirstNet-approved minimum set of voice and video CODECs.

4.5.4 UE Battery Life

Battery life is a particularly important element for portable devices that will operate in the public safety environment. Batteries must be able to provide operability for a typical “shift” that a user works. The duration of a shift can vary greatly. A common duration is 8 to 10 hours. Devices should be designed with the highest battery capacity possible. Devices that allow user swap out of battery packs would be the ideal to allow continuous operations in the field.

4.6 Local Operations Support

This section is concerned with public safety’s need for operational controls for, and visibility into the NPSBN. PSEs cover a full spectrum from large, local, tribal, state, or federal organizations with professional operations staffs, to small, rural, and volunteer organizations without such capabilities.

Large PSEs that have their own operations systems have a strong desire to integrate those existing systems with corresponding systems of the NPSBN. For example, states that maintain statewide radio systems and operate network operations centers for those systems, wish to leverage that investment and incorporate monitoring of the relevant portions of the NPSBN.

At the other end of the spectrum, small organizations still need to “turn the knobs” and see into the network, but often do not have capital resources to invest in integration of their existing, often very basic, tools with the NPSBN. These organizations need the NPSBN to provide O&M tools (e.g., web portals or other applications) to provide the control and visibility they need for their operations.

In particular, public safety requires the following important O&M capabilities:

- Some public safety organizations need the NPSBN to provide interfaces based on publicly available standards that allow integration of their existing O&M[13] systems with corresponding NPSBN O&M capabilities.
- Some public safety organizations require the NPSBN to provide simple, easy-to-use tools to access those same NPSBN O&M capabilities.
- Among the O&M capabilities that public safety needs the NPSBN to provide are: provisioning and management of NPSPN Users (NPSBN-U) and PSE O&M users, access to detailed, current, and historical billing and usage information.

Table 69: General Network Management Requirements

#	Requirement
1	The NPSBN O&M solution SHALL provide provisioning and management of NPSBN Users (NPSBN-U).
2	The NPSBN O&M solution SHALL provide access to detailed, current, and historical billing and usage information per Section 4.6.9.

The following subsections provide more specific requirements for local operations support.

4.6.1 O&M Personnel Management

Like any enterprise, PSEs experience personnel changes, vacations, and so on that affect the rights and privileges of their administrative staff. These changes are not infrequent and are often time-critical. PSEs, therefore, SHOULD have the ability to directly manage the authority, with regard to NPSBN systems, of their administrative and management users.

4.6.2 Network Management

Network management is key to ensuring network and service reliability/availability for first responders. This section describes the network management services and associated interfaces required of the NPSBN.

4.6.2.1 Network Management Users

To identify the required set of NPSBN network management services, it is important to define the user context associated with NPSBN and PSEN network management.

The context of each O&M user as it relates to network management is defined below:

- The FirstNet O&M user is solely concerned with managing and monitoring the FirstNet infrastructure, specifically the FirstNet Core, RAN, transport network, backhaul, and national broadband application servers. This user is out-of-scope for this document.

[13] Per the reference model, "O&M" refers to configuration, device management, network monitoring, security management, and other functions related to Operations and Maintenance of the system.

- The PSE O&M user is concerned with managing and monitoring all infrastructure associated with the PSE. This includes NPSBN RAN infrastructure scoped to the PSE domain, critical NPSBN CORE infrastructure, PSEN infrastructure, and PSE-based application servers. This user is the primary user of network management services.

4.6.2.2 Integration into Existing PSE Network Management Systems

A PSE operations staff might choose to integrate the monitoring of their existing PSEN infrastructure and the NPSBN scoped to their PSE into the PSE's existing network management system. In this case, integration of network management streams between the PSE-scoped NPSBN and PSEN must be supported.

4.6.2.3 Remote Monitoring via NPSBN O&M Tool

Alternatively, the PSE operations staff might choose to monitor the NPSBN and PSEN infrastructure separately. In this case, integration of network management streams between the PSE-scoped NPSBN RAN and the PSEN is not necessary. Instead, O&M tool access to the NPSBN network management capabilities will be sufficient for the PSE O&M users chartered with monitoring the portion of the NPSBN scoped to their PSE. The O&M tool should allow for communications between O&M tool users (e.g., online user forum) and communications to FirstNet support staff (e.g., online help chat).

4.6.2.4 Fault Management

To support both operations patterns described in Sections 4.6.2.2 and 4.6.2.3, the NPSBN must provide basic fault management capabilities:

The NPSBN must coordinate planned NPSBN outages with the PSEs, especially for the NPSBN RAN and backhaul associated with the PSE. An administrative process must be established between the NPSBN and the PSE to formalize coordination and authorization of PSE-scoped NPSBN RAN and backhaul outages. Polices and standards on a national level are referenced in Section 3.3. Following are requirements for fault management.

Table 70. Fault Management Requirements

#	Requirement
1	The NPSBN SHALL have the ability provide an alarm stream to each PSE, scoped to network/service outage-level events.

4.6.2.5 Performance Management

To support both operations patterns described in Sections 4.6.2.2 and 4.6.2.3, the NPSBN must provide two distinct performance management capabilities:

- A secure performance management interface scoped to the PSE (e.g., database query, file transfer, etc.).

- An O&M Tool interface to the NPSBN performance management system secured with the appropriate authentication/authorization controls. The O&M Tool should allow an authorized PSE O&M User to view RAN and backhaul performance data.

Following are requirements for performance management.

Table 71. Performance Management Requirements

#	Requirement
1	The NPSBN SHALL provide a secure performance management interface scoped to the PSE.
2	The NPSBN SHALL provide performance data scoped to the PSE.
3	The NPSBN SHALL provide an O&M tool interface to the NPSBN performance management system secured with the appropriate authentication and authorization controls.

4.6.3 User Setup, Add, Change, Delete, and Group Users

Local operations PSE administrators must be able to perform the initial setup required to add a user to the NPSBN system. Once setup, PSE administrators must be able to change the attributes of the users, suspend users, and remove users. For example, all resources assigned to the Rapid Response Team, Engine 1, or Car 54. Following are user setup requirements for PSE administrators.

Table 72. PSE Administrator User Setup Requirements

#	Requirement
1	Each PSE administrator SHALL have the ability to add new users to the discipline they are responsible for via a local interface (e.g., in a large local administration area, one administrator might setup only the Fire Department personnel while another administrator sets up only the Police Department personnel).
2	Each PSE administrator SHALL have the ability to change the attributes of the users, suspend users, and remove users they are responsible for via a local interface.
3	The User setup interface SHALL allow for an API interface that will process TXT, CSV, or XML files to facilitate bulk provisioning.

4.6.4 Device Setup, Add, Change, and Delete

As part of the user setup, the PSE administrator will need to define the types of devices the user is authorized to use. This setup will not tether a user to a specific device but will define which types of devices the user is authorized to log onto. The logging process will tether the user to a particular device for the duration of the session (e.g., the initial logging onto the mobile platform in the patrol car at the beginning of the shift). Additional device management requirements can be found in Section 4.2.10. Following are device setup requirements for PSE administrators.

Table 73. PSE Administrator Device Setup Requirements

#	Requirement
1	Each PSE administrator SHALL have the ability to define the types of devices the user is authorized to use.
2	Each PSE administrator SHALL have the ability to remove the assignment of certain types of devices the user is authorized to use.
3	Each PSE administrator SHOULD be able to select from a group of predefined roles that will populate a full set of standard devices authorized for that role.
4	The user setup interface SHALL allow for an API that will process TXT, CSV, or XML files to facilitate bulk provisioning.

4.6.5 Application Setup, Add, Change, and Delete

In addition to user and device setup, the PSE administrator will need to configure the allowable set of applications for the user and to establish any role specific parameters for the application. Following are application setup requirements for PSE administrators.

Table 74. PSE Administrator Application Setup Requirements

#	Requirement
1	Each PSE administrator SHALL have the ability to define the applications (NPSBN deployed, PSEN deployed, or 3rd party deployed) the user is authorized to use. In addition, the setup may require role-specific settings that the PSE Administrator needs the ability to modify (e.g., they can use an application but just in read-only mode).
2	Each PSE administrator SHALL have the ability to change the authorized applications and their settings.
3	Each PSE administrator SHALL have the ability to remove the authorization to access an application.
4	The user setup interface SHALL allow for an API that will process TXT, CSV, or XML files to facilitate bulk provisioning.

4.6.6 Problem Ticket System to Report a User, Device, or Application Setup Issue

The PSE administrator will need a way to manage the problem resolution process. Part of the administrative interface with the NPSBN network will be for problem resolution. In keeping with the original user setup, the problem resolution functions have been broken into those related to user, device, and application setup. It is more beneficial to have the problem management system accessible to the user; however, the PSE administrator will also need access and the ability to create problem tickets directly.

The PSE administrator will need to initiate and track problems associated with incorrect user data or requests for change that cannot be handled immediately. In addition, the PSE administrator will need to report problems in the actual system itself as it relates to user setup. Following are user problem reporting requirements for PSE administrators.

Table 75. PSE Administrator User Problem Reporting and Resolution Requirements

#	Requirement
1	Each PSE administrator SHALL have the ability to create new problem tickets related to the user device, and application setup process.
2	Each PSE administrator SHALL have the ability to track the progress of a user, device, and application problem ticket and to provide input along the way.
3	Each PSE administrator SHALL have access to summary data that will show the progress on all tickets for the PSE and for those that they have initiated or those which relate to a specific user under their authority.

4.6.7 Device Replacement Process

If a problem arises with a piece of hardware and it is required for the user to be able to perform their duties, then spare replacement devices must be available on site. The management of the provisioning process must be under control of the PSE administrator because the administration of the replacement device pool under the control of the administrator and the tracking of device availability would been done using the problem ticket management process. In other words, the problem management system would be set up with an initial number of devices. When those devices are used for replacements, they show as assigned, not available as replacement. The PSE Administrator console would have a section reporting on the “health” of the replacement pool. Note: the replacement pool is not the same as the cache; they are two completely separate sets of equipment and should not be blended. Radio caches are for distribution to temporary resources brought in to assist in an incident. Following are device replacement requirements for PSE administrators.

Table 76. PSE Administrator Device Replacement Requirements

#	Requirement
1	Each PSE administrator SHALL have the ability to record in inventory, assign, and track devices in the local replacement pool.
2	Each PSE administrator SHALL have the ability to view the status of all devices in the pool and to get proactive warnings when the pool is critically low.

4.6.8 Dynamic Role Re-Assignment

The PSE administrator must be able to re-assign roles (i.e., from a regular role to an incident role) for individual users dynamically. As part of the normal incident declaration process and the assignment of

NIMS roles, the individuals in those roles must have their settings changed in the user setup tables. Following are requirements for dynamic role re-assignment.

Table 77. Dynamic Role Re-Assignment Requirements

#	Requirement
1	Each PSE administrator SHALL have the ability to change the role of a user for incident management purposes and to have that change propagate through the system to ultimately change the priority levels for the device to tower connection and the role within application access and priority.
2	Each PSE administrator SHOULD have the ability to reset individual users to the pre-incident setting in a one-step action.

4.6.9 Billing Interface

The local PSEs (jurisdictions) are best suited to manage their own staff and to manage their billing and usage reporting options. This section describes the required set of capabilities needed by a PSE Administrator or PSE Customer Service Representative for the NPSBN Billing Interface.

Table 78. PSE Administrator Billing Setup Requirements

#	Requirement
1	The NPSBN SHALL provide an O&M tool.

4.6.9.1 Reporting of User, Device, and Application Billing Information to the PSE

An electronic report of billing of each agency's users, devices, and applications that make up the ultimate billing model used by FirstNet must be provided to each PSE. The electronic report should be in a PDF format and common open standard softcopy formats such as CSV, XML, and TAP3 so agencies can conduct analysis on their devices and users. The information shall be of sufficient detail so the agency can reconcile to the billing questions and requests from PSE management and in billing disputes with NPSBN.

FirstNet should provide an interface to transaction and billing information at no charge to the local PSE. FirstNet should reconcile all billing activity with its commercial carrier partners and national public safety applications on behalf of the PSEs. FirstNet should also provide commercial and application level integration capability. In other words, provide billing data in a standard electronic format for entry into existing billing and accounts payable systems.

PSE should have access to transactions for their activity at the level equivalent CDRs but in a uniform, vendor-neutral format. FirstNet should provide sufficient billing detail for transport, multicarrier roaming, and application level usage to allow local administrator invoice validation. In other words, enough detail so that the local administrator can calculate and validate the invoice totals directly. Following are PSE requirements for reporting user, device, and application billing information.

Table 79. Reporting of User, Device, and Application Billing Information to the PSE

#	Requirement
1	The NPSBN Billing Interface SHALL supply user, device, and application billing information in PDF and open standards formats (CSV, XML, TAP3, etc.).
2	The NPSBN Billing Interface SHALL reconcile all billing activity with its commercial carrier partners and national public safety applications on behalf of the PSEs.
3	PSE SHALL have access to transactions for their activity at the level equivalent CDRs but in a uniform, vendor-neutral format.
4	The NPSBN Billing Interface SHALL provide sufficient billing detail for transport, multicarrier roaming, and application level usage to allow local administrator invoice validation.
5	The NPSBN Billing Interface SHALL provide commercial and application level integration capability.
6	The NPSBN Billing Interface SHALL supply an interface for PSEs to query up-to-date billing detail at will.

4.6.10 Device Management Interface

This section addresses device services that can be managed by the PSE administrator. It presupposes that an interface has been provided that will allow for device management functions on a PSE-wide basis. This section is concerned with the local operations of the user, including how certain services are accessed and who can use such services. It describes those services that can be enabled or not be enabled by an approved administrator and it addresses any particular interface requirements with services or features.

A local authorized PSE Administrator (i.e., a local public safety enterprise administrator, official from a PSAP, emergency management agency/operations center official, or a communications leader at an incident) would typically have responsibility for network administration, wireless communications, and/or systems management. The PSE Administrator would work within the device hardware/software framework and manage certain system features and functions consistently across their entire local/agency user base according to predetermined roles/responsibilities. They would typically also have the responsibility for addressing quality of service issues or outages in response to end-user notification of such issues.

Table 80. Device Management Local O&M Requirements

#	Requirement
1	A PSE O&M administrator SHALL have the ability to add devices quickly and efficiently without coordination with others.
2	A PSE O&M administrator SHALL have the ability to configure the device remotely.

#	Requirement
3	A PSE O&M administrator SHALL have the ability to push software upgrades/updates.
4	A PSE O&M administrator SHALL have the ability to install additional applications.
5	A PSE O&M administrator SHALL have the ability to control access to the device.
6	A PSE O&M administrator SHALL have the ability to authenticate users.
7	A PSE O&M administrator SHALL have the ability to implement and manage security features (e.g., encryption, firewalls, anti-virus, VPN connection, and strength of authentication).
8	A PSE O&M administrator SHALL have the ability to remove applications and/or deactivate device applications.

Public Safety Users, Secondary Users, and Application Users are those individuals "in the field/at the scene" using the hardware/software he or she is enabled and authorized to use on the job. These users would have the ability, within certain limits set by the system or PSE Administrator, to access, enable, or otherwise use certain services, features, or applications. Those may be local agency applications or applications made available across the system by the NPSBN. Following are device management requirements for local public safety users.

Table 81. Device Management Local Public Safety User Requirements

#	Requirement
1	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to download software, web links, and/or shortcuts to the device.
2	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to set passwords and other security features on their device.
3	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to enable Wi-Fi and Bluetooth features as required.

4.7 Migration and Evolution

Requirements that enable a smooth migration of current public safety data applications will encourage broad adoption of the NPSBN. This can only serve to maximize interoperability and help to ensure the network's success.

This section recommends technical requirements to facilitate the migration of public safety users' and agencies' existing data applications from their current data systems or services to the NPSBN. This section also addresses technical requirements associated with the evolution of the NPSBN itself.

4.7.1 Migration of Cellular Service Features

The principal driver for migration from commercial cellular systems is to encourage public safety entities to use the NPSBN. However, it is recognized that a large number of public safety entities use commercial cellular service providers to support applications present in their PSENs. It has been identified that in future phases, design considerations should include the goal of a ubiquitous nationwide network.

Following are requirements for migrating cellular service features to the NPSBN.

Table 82. Comparable Commercial Service Feature Requirements

#	Requirement
1	The NPSBN SHALL support public safety applications, either by providing subscribers a means of connecting to their home PSENs, or by providing common nationwide applications, or both.

4.7.2 Technology Evolution

This section provides requirements focused on evolution and upgrades of the network. The topic areas include roadmap and feature planning, configuration management, upgradability and backwards compatibility, life-cycle management, coverage and capacity management, network availability management, and network security management.

4.7.2.1 Upgradability and Backward Compatibility

The objective of upgradability requirements is to minimize impacts of software upgrades on hardware. However, some system features such as higher-order multiple-input and multiple-output (MIMO) and enhanced Multimedia Broadcast Multicast Service (eMBMS) will require deployment of new and/or additional hardware. Following are NPSBN requirements for backward compatibility.

Table 83. Upgradability and Backward Compatibility Requirements

#	Requirement
1	The infrastructure equipment SHALL be backwards compatible (e.g., n -2) for required interfaces. FirstNet SHALL identify and manage interfaces that are required to maintain backwards compatibility across upgrades.

4.7.2.2 Coverage and Capacity Management

Following are NPSBN requirements for coverage and capacity management.

Table 84. Coverage and Capacity Management Requirements

#	Requirement
1	The RAN, EPC, and transport equipment SHALL support capacity expansion of existing equipment or addition of new elements while minimizing out-of-service time.

4.7.2.3 Availability Management

Following are NPSBN requirements for availability management.

Table 85. Availability Management Requirements

#	Requirement
1	The RAN, EPC, and transport equipment SHALL support capabilities to add redundant components while minimizing out-of-service time.

4.7.2.4 Location Technology Evolution

Future public safety networks should meet minimum location information requirements, and strive to leverage commercially deployed technologies in order to achieve a broad level of location service compatibility. However, commercially deployed location methods and/or technologies may not be able to meet all public safety requirements. Public safety applications may impose additional location service requirements beyond those offered by commercial wireless providers in the following example areas:

- High-volume location updates
- High accuracy
- Many applications require access to location information
- Strong security

A variety of public safety applications require the capability to collect and convey user location data in real time. In addition, location data should be accessible to appropriate applications and only to the appropriate users or administrators. Location data applications may reside in multiple platforms, such as:

- NPSBN-U devices
- Regional and/or agency level applications data networks
- National-level application data networks

The LTE standards support several methods of locating devices using GPS or network-assisted determination methods. Network-assisted methods are not limited to LTE; these methods also support 3G and Wi-Fi access networks. However, the full breadth of these methods is typically not implemented in commercial wireless networks, and the consumer-oriented use cases can stress the location technologies in different dimensions. For these reasons, the public safety location requirements referenced in the preceding paragraphs may need to be part of an evolution plan for the network services layer. Support for E9-1-1 Phase II (i.e., inclusion of latitude and longitude) location services will require evolved location services. Lastly, public safety will require location service availability while roaming on commercial wireless networks and may be required to provide location services for secondary users and/or commercial inbound roamers. Following are requirements for location technology migration.

Table 86. Location Technology Migration Requirements

#	Requirement
1	The NPSBN location service SHALL provide location information associated with NPSBN users.
2	The NPSBN location service SHALL support authorization for access to NPSBN users' location information.
3	NPSBN-U location information SHALL be available to PSEN hosted applications
4	NPSBN-U location information SHALL be available to applications hosted via NPSBN Services.
5	The NPSBN location service SHALL support strong security between location clients and servers.
6	The NPSBN location service SHALL support receiving location information from NPSBN users while roaming.

Intentionally Blank

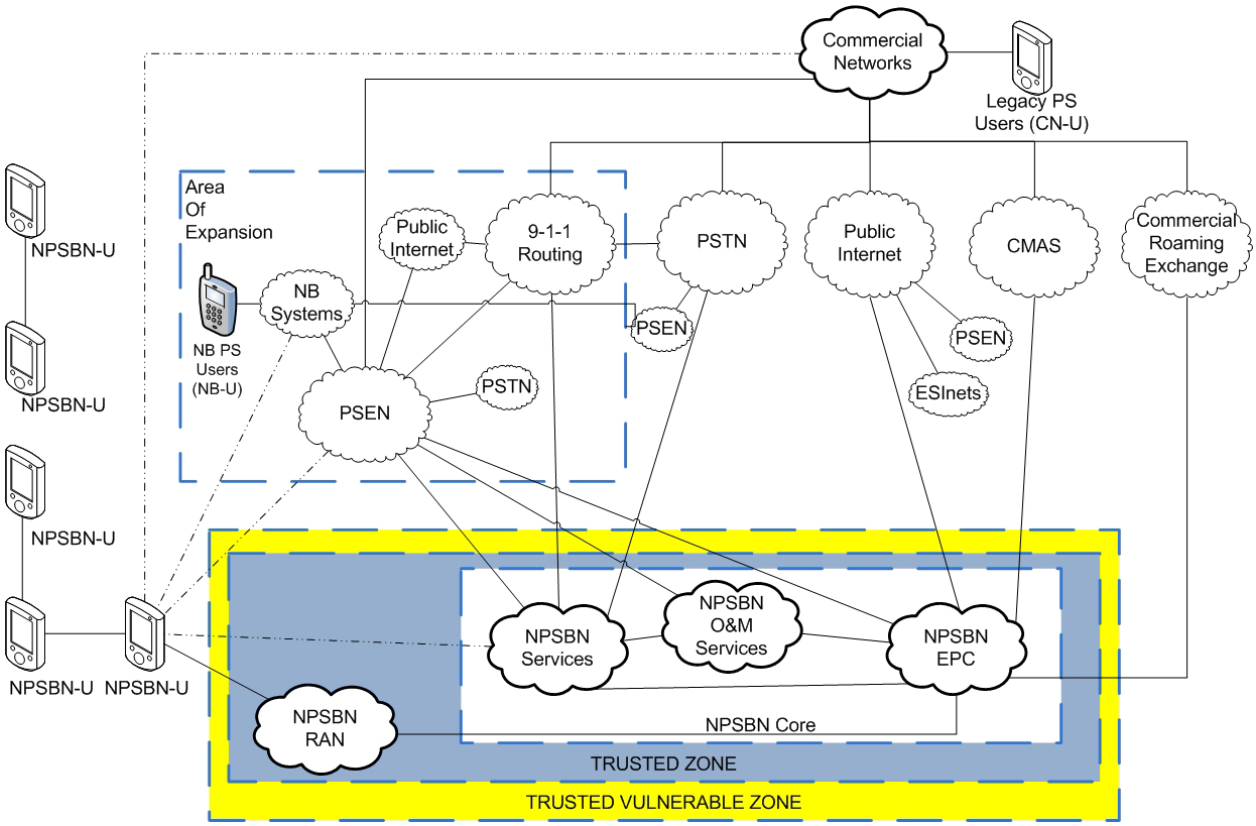
5 Security Requirements for the NPSBN

Secure communications are a core requirement for the NPSBN. The NPSBN security requirements include but are not limited to: user credentialing and access control, authentication, auditing, confidentiality, data integrity, physical security and control, the definition of acceptable resources, and applications.

This section describes security requirements for the overall NPSBN network. These security requirements include services, device management, and an identity management framework. More generally for the purposes of this SoR, "Network Services" comprise capabilities provided by the NPSBN to facilitate the interoperation of user services and applications by providing a common infrastructure for oft-used or shared information or functions, or by providing a standard means of manipulating information within the NPSBN.

These services can be provided by a central authority in support of NPSBN-Us, delivered through either centralized or distributed service mechanisms. In addition, there are significant security requirements to consider at the network services layer, which this section discusses. Figure 5 illustrates the concepts of a 'trusted zone' and a "trusted vulnerable zone."

Figure 5. NPSBN Reference Architecture with Trusted Zone



In ITU-T X.800 [9] typical attacks or threats against a network communication system are categorized in five basic categories:

- **Destruction:** the destruction of information or communications such that it can no longer be used. An example would be terrorists destroying the NCIC criminal database such that law enforcement officers could no longer make lookups. This attacks the availability of information.
- **Corruption:** the changing of information such that it is no longer accurate. An example would be a criminal changing a felony conviction in a state database to reflect instead a misdemeanor. This is attacking the integrity of the information.
- **Removal:** the removing of information so that it cannot be accessed, but it is not destroyed. An example would be a terrorist removing the information from the U.S. Center for Disease Control on how to deal with a bird-flu pandemic, such that the information would no longer be available to EMS first responders. This attacks the availability of information.
- **Disclosure:** releasing confidential information. An example is a hacker group exposing the identities of drug investigation informants and the law enforcement undercover agents working with them. This attacks the confidentiality of information.
- **Interruption:** interfering with communications such that legitimate users cannot get their messages through in a timely manner. An example would be someone jamming fire department radio transmissions while a two-alarm fire is underway, such that the IC cannot get communicate adequately with the fireground units. Another example would be for a criminal to disconnect the IP data line coming into a sheriff's office to prevent the personnel inside from having access to criminal files. This attacks the availability of information.

Security at every layer of the system needs to consider these threats and provide the appropriate protection for the NPSBN-U users and infrastructure to reduce the exposure of the network and its operations. This document considers security at each of the three following layers:

- **User Services (Section 4.1):** is where NPSBN-U access specific software applications in performing their duties (e.g., software applications like the Integrated Automated Fingerprint Identification System(IAFIS) for law enforcement fingerprints, or the National Fire Incident Reporting System(NFIRS), or state EMS field medical reports).
- **Network Services (Section 4.2):** is where a variety of services provide the framework for the above mentioned User Services to be delivered to a public safety user throughout the infrastructure. Network services transcend any specific application or user device. For example, the use of a common identity management framework across the network for identification of who, what, and where the user is located is a Network Service. This section describes a security framework that provides a network service.
- **Transport Services (Section 4.3):** focus on the specific components or protocol mechanism in the network that carry information and provide the transport infrastructure for delivery of packets to the various components of the network. (Example transport components: eNodeB,

gateways, routers, servers, switches, fiber optic links, microwave radio links, satellite links, and other telecommunication components.)

Depending on where a particular device, component, or user is within or external to the NPSBN determines what the security impact and considerations for the specific component should be. The system will require visibility and configurability in the security design of the system. This document is concerned only with the NPSBN requirements and any requirements that exist in the interfaces between the NPSBN and other architecture components such as Public Safety Enterprise Networks(PSEN).

5.1 Security Policy

The transition to the NPSBN will require security policies and procedures to access information. Although many of the users will have experience with personal smartphone devices, stricter security policies for the NPSBN will be needed. The security policy should also address administrative security planes including:

- Management Plane of infrastructure and devices
- Control Plane of infrastructure and devices
- User Identity Plane
- User Data Plane

Following are security policy requirements for the NPSBN.

Table 87. Security Policy Requirements

#	Requirement
1	FirstNet SHALL define an NPSBN security policy for information protection and security requirements to ensure confidentiality, integrity, and availability of information in-transit and at-rest for NPSBN applications and services.
2	FirstNet SHALL define an NPSBN security policy for monitoring, logging, and data retention policies for NPSBN applications and services.

5.2 Security Management

Following are requirements for security management.

Table 88. Security Management Requirements

#	Requirement
1	FirstNet SHALL define a policy to insure that the NPSBNSHALL support capabilities to respond, in near real-time, to security threats without incurring a service outage.

#	Requirement
2	FirstNet SHALL define a policy to insure that updates to security management will not compromise existing security measures.
3	FirstNet SHALL define a process for the safe disposal of UE equipment once end of life is reached to protect again inadvertent loss of data.
4	The RAN, EPC, and transport equipment SHALL support capabilities to respond, in near real-time, to security threats.
5	Updates to security management SHALLNOT compromise existing security measures.

5.3 Information Assurance

Two of FirstNet's many information assurance roles are to protect the NPSBN against and monitor for cyber attacks. This protection includes user services and NPSBN-hosted applications in addition to the network infrastructure. To meet these needs, applications will need to comply with FirstNet information assurance practices and policies.

Following are information assurance requirements for NPSBN-hosted applications.

Table 89. Information Assurance Requirements for NPSBN-Hosted Applications

#	Requirement
1	Applications hosted on the NPSBN SHALL comply with all NPSBN information assurance procedures, policies, and requirements.
2	PSEs SHALL be allowed to provide additional layers of security if desired.
3	FirstNet's security policy for user services and NPSBN-hosted applications SHALL require users to securely authenticate for access.
4	FirstNet's security policy for user services and NPSBN-hosted applications SHALL provide and maintain anti-malware and anti-virus protection.
5	FirstNet's security policy SHALL require applications and user services to be secure against intrusion.
6	FirstNet's security policies SHALL require applications hosted in PSENs to comply with clearly documented security policies and procedures designed to protect PSEN and NPSBN infrastructure from cyber attack, loss, or exposure of sensitive information.

5.4 User Services Security

User services security operations requirements refer to the protection of the user services components and infrastructure from cyber attack, loss, and exposure of sensitive information. Following are user services requirements for security operations.

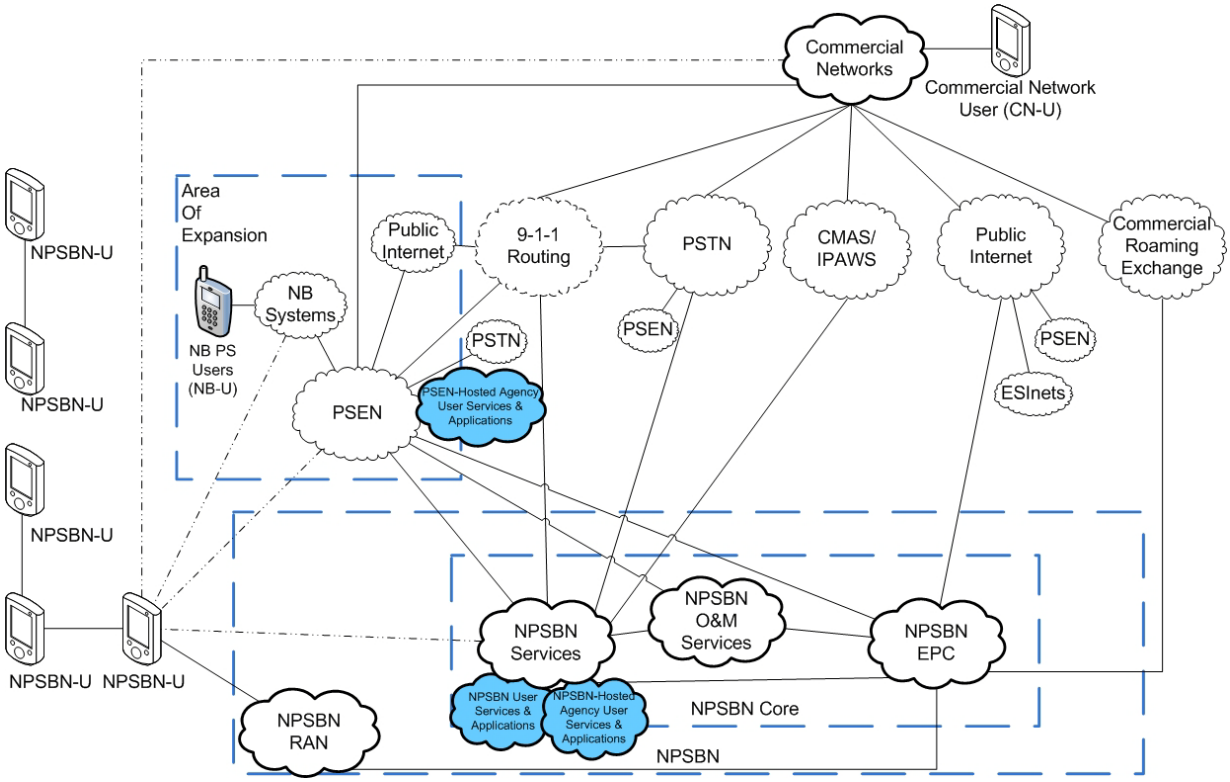
Table 90. User Services Security Operations Requirements

#	Requirement
1	The NPSBN SHALL protect user services infrastructure to ensure localities, regions, or the nationwide services are not impacted by various cyber attacks scenarios.
2	The NPSBN SHALL protect user services infrastructure against corruption or unauthorized modification (e.g., software, configurations, etc.).
3	The NPSBPN SHALL periodically verify that the user services infrastructure and hosted applications servers do not present security vulnerabilities.
4	NPSBN user services SHALL meet public safety-grade availability and reliability requirements.

5.5 User Authentication for User Services and Hosted Applications Access

This section outlines the requirements for authenticating users for access to NPSBN-provided user services and applications, NPSBN-hosted public safety agency-provided applications, and PSEN-hosted public safety agency-provided applications. Figure 6 shows the locations and relationship of the different hosting options, which are further explained in Hosted Applications.

Figure 6. Hosted User Services



It is expected that the NPSBN will supply an authentication mechanism to validate both the device (e.g., through the use of SIM/UICC) and the user. FirstNet should define an identity framework that allows for users of the network to manage a single identity credential to authenticate throughout the network. Agencies might have applications they access over the NPSBN and these requirements do not force them to modify these applications. Agencies could benefit from the ease of using a single user authentication mechanism for both PSE and FirstNet deployed applications.

Following are NPSBN identity management requirements for user interaction.

Table 91. Identity Management for User Services and Applications

#	Requirement
1	The NPSBN SHALL provide user services and applications hosted on the NPSBN access to the NPSBN identity management framework.
2	NPSBN user services and applications SHALL use the NPSBN identity management system.
3	NPSBN-hosted agency applications SHALL use the NPSBN identity management system.
4	PSEN-hosted applications SHALL be allowed to use the NPSBN identity management system.
5	PSEN-hosted applications SHALL NOT be required to use the NPSBN identity management system.

#	Requirement
6	The NPSBN SHALL permit the use of last-used credentials to allow the set up of emergency calls without due course to the usual authentication process.

Following are requirements for user access control.

Table 92. Access Control Requirements

#	Requirement
1	The NPSBN SHALL support the ability for a PSE O&M user to restrict access to NPSBN user services based on a user's identity and role.
2	The NPSBN SHALL support the ability, based on a user's identity and role, to limit access to PSEN-hosted user services, if configured by the PSEN to use the NPSBN identity management framework.
3	The NPSBN SHALL support the dynamic modification of access control settings in emergency support situations requiring a configuration modification of access controls (automated or manual).
4	The NPSBN SHALL have the ability to shut off access to all or individual user services components or interfaces based on detected illegal or illegitimate activities, or when activities are deemed a threat to the operation and safety of the network.
5	The NPSBN SHALL require all user services devices, servers, and other components that are part of the operational infrastructure to be monitored and operated within an established set of security policies.

5.6 Messaging Security

A number of security related topics are relevant to messaging. Messaging technologies are associated with a variety of security threats, ranging from spam to embedded malware that have the potential to corrupt or steal sensitive user data. The messaging service and NPSBN must provide mechanisms to protect against such threats.

Users of the NPSBN also have the need in some circumstances for identity hiding. For example, a NPSBN-U communicating with a user on the public Internet, in some instances, may need a mechanism by which messages can be exchanged but the public Internet user is not left with the ability to send messages to the NPSBN-U at a subsequent time, or even distribute the NPSBN-U's address information to others without the NPSBN-U's knowledge or permission.

Note that public safety messaging usage may differ significantly from normal commercial usage. Care needs to be taken to avoid filtering messages whose characteristics are valid for usage by public safety but would appear suspicious and trigger filtering on a commercial network.

Following are security requirements for messaging at initial launch.

Table 93. Messaging Security Requirements

#	Requirement
1	NPSBN-Us SHALL be authenticated prior to accessing the text and multimedia messaging service.
2	NPSBN-Us SHALL be suitably authorized prior to accessing the text and multimedia messaging service.
3	The messaging service SHALL provide confidentiality for text and multimedia messaging (both message content and related control).
4	The NPSBN SHALL provide the capability to filter spam and other undesirable text and multimedia messages as per configured policy.
5	The NPSBN SHALL provide the capability to detect text and multimedia messaging infected with malware and prevent its delivery to the intended target.
6	Authorized administrators SHALL have the ability to configure the content types (e.g., attachment file types, MIME types, program files, etc.) that are permitted for messaging content by their associated NPSBN-Us.
7	The messaging service SHALL have the ability to “whitelist” messaging contacts. The intention is to provide the capability to add contacts to a white list, which will ensure that their messaging communications are allowed delivery to NPSBN-Us (e.g., not deleted by filtering).
8	The messaging service SHALL have the ability to “blacklist” messaging contacts. The intention is to provide the capability to add contacts to a blacklist, which will ensure that their messaging communications are not allowed delivery to NPSBN-Us.
9	The filtering mechanisms used by the NPSBN to protect NPSBN-Us and their associated devices from spam and malware-infected text and multimedia messages SHALL be capable of adapting to the special needs of public safety. The intention is to note that public safety messaging usage may differ significantly from normal commercial usage. Care needs to be taken to avoid filtering messages whose characteristics are valid for usage by public safety but would appear suspicious and trigger filtering on a commercial network.

5.7 Security Operations

Security operations refers to the responsibility of the NPSBN network services component to protect the network components and infrastructure within the trusted zone from cyber attack, loss, and exposure of sensitive information, and from other threats to the security and reliability of the system that may

impact either the network itself (NPSBN), the users of the network (NPSBN-U), or the mission of the agencies employing the network services. Following are requirements for security operations.

Table 94. Security Operations Requirements

#	Requirement
1	The NPSBN SHALL provide the necessary level of transport, device, and application security monitoring and boundary protection service at all connection points, external interfaces and infrastructure devices in order to assure either NPSBN or the PSEN networks are not impacted by various cyber attacks scenarios. Note: The Federal Information Security Management Act (FISMA) may be used to help identify the necessary levels for protection of the NPSBN.
2	The NPSBN SHALL provide a health and status report of the security posture of the network and indicate how that status impacts overall operational availability.

5.8 Boundary Protection Services

The requirements for boundary protection focus on specific activities related to protecting the trusted zone from un-trusted network and system interfaces using the trusted but vulnerable zone as a connection point. As the cyber threat changes the technology and implementation of boundary protection systems change and require more sophistication and analysis capabilities, the requirements to protect the NPSBN remain very predictable. Following are service requirements for boundary protection.

Table 95. Boundary Protection Service Requirements

#	Requirement
1	The NPSBN SHALL be able to immediately shut down a boundary between a locality or agency for purposes of protecting the NPSBN network from attack or possible damage.
2	The NPSBN SHALL provide the ability to limit or prohibit certain access to websites, applications, or other data types at the boundary based on the known cyber threats to the NPSBN without impacting the mission operations of NPSBN-Us not using those specific services.
3	The NPSBN SHOULD provide a status and information interface to the PSE administrators in a locality or agency responsible for a PSEN that any particular boundary device is between.
4	The NPSBN SHALL have the ability to alert any PSENs, NPSBN-Us, or PSEs of illegal, inappropriate, or problematic boundary activities.

5.9 Malware, Virus, and Zero Day Detection

The requirements for malware, virus, and zero day detection focus on specific activities related to protecting the trusted zone from the risks associated with malware and viruses that could potentially impact NPSBN operations, or put at risk the data privacy of users, or create the opportunity for corruption of mission operational data. As the cyber threat changes the technology and implementation of malware and virus protection systems may change, but the requirements to protect the NPSBN and its components remain identifiable. Following are requirements for malware, virus, and zero day detection.

Table 96. Malware, Virus, and Zero Day Detection Requirements

#	Requirement
1	The NPSBN SHALL monitor all common infrastructure components, servers, routers, gateways, and other vulnerable equipment using appropriate malware and virus protection mechanisms.
2	The NPSBN SHALL use monitoring tools to detect and analyze the various delivery methods used for distribution of malware, bugs, and virus software over including SMS, MMS, email, and other applications.
3	The NPSBN SHALL provide protection of any shared services applications to assure they are safe from malware, virus, and zero day infestations.

5.10 Network Component Security and Policy Management

The security requirements for network components and policy management focus on specific requirements for protecting the trusted zone component from illegal or illegitimate access, unintended or illegal modification of components, and from unintended consequences from the loss or misplacement of devices. Following are security requirements for network components and policy management.

Table 97. Network Component Security and Policy Management Requirements

#	Requirement
1	The NPSBN SHALL provide the ability to set policy or limit access to any component or device accessing the trusted portion of the network according to their role and according to NPSBN policy.
2	The NPSBN SHALL consider all UEs as untrusted and shall enforce security policies that protect NPSBN assets from UEs.
3	The NPSBN SHALL provide the ability to shut down access to any component or NPSBN-U either internal to the NPSBN or to external interfaces deemed a threat to the operation and safety of the network as determined by a set of security parameters and protocols.

#	Requirement
4	The NPSBN SHOULD notify the appropriate agency or locality of any rogue device or devices deemed improper allocated to that agency PSEN.

5.11 Internet Access Service Monitoring

No single interface to the NPSBN will present a greater risk to the operation of the network then the connections to the public Internet. However, the public Internet offers an incredible amount of benefit and opportunity to the NPSBN-Us through access to applications and data content. The internet access service monitoring requirements focus on protecting the trusted zone of the NPSBN from the risks associated with connectivity to the public Internet either with the trusted zone or external to the trusted zone (e.g., within the PSEN). Typical enterprise operations protect the traffic, data, and application interfaces traversing over their boundaries between the enterprise and the public Internet. According to these NPSBN cyber security requirements, the systems must be in place to both allow proper access and data traversal of Internet traffic, as well as restrict access and limit data traversal as determined by policy. It is anticipated that the specific implementation and technologies used to accomplish these requirements will change over time, but the requirements are very predictable and important in reducing the risk to the NPSBN. Following are service requirements for Internet access.

Table 98. Internet Access Service Monitoring Requirements

#	Requirement
1	The NPSBN SHALL monitor and protect against threats at any provided Internet access points within the NPSBN trusted zone whether the access is for internal NPSBN users or for providing access to mobile NPSBN-Us.
2	The NPSBN SHALL prohibit the connection or use by any device, server, or component within the trusted zone of an unrestricted or unmonitored public Internet access connection.
3	The NPSBN SHALL allow PSENs to provide Internet access to their users as long as the boundary protection guidelines between the NPSBN and the PSEN are followed and adhered to.
4	The NPSBN SHALL have the ability to restrict or even terminate the public Internet connections to the trusted network if it is deemed that the public internet has become a threat to operations.

5.12 Network Monitoring, Logging, and Analytics

The network monitoring, logging, and analytics requirements focus on the monitoring of network traffic, information logging, and forensic analytics of information with a purpose of protecting the trusted zone of the NPSBN from the risks associated with illegal access, denial of service attacks, and other external cyber threats. In addition, the information will assist in any situations of internal illegal or improper activity, or where forensics activities may requirements information about network logins, control

commands, equipment access, etc. Following are the NPSBN requirements for monitoring, logging, and analytics.

Table 99. Network Monitoring, Logging, and Analytics Requirements

#	Requirement
1	The NPSBN SHALL store and monitor access logs that provide information on the identity of access devices, agency, role, and location.
2	Access to the stored data SHALL be limited on a need-to-know basis and within the proper access rules dictated by policy.
3	The NPSBN SHALL store and monitor transport device traffic, configurations, and information necessary for both analytics and forensics used in protecting the network assets from cyber threats.
4	The NPSBN SHALL have a set of tools for analyzing and monitoring system and user log data to determine possible threats to the network before they occur or to support post-event activities.

5.13 Access Control

The requirements for access control speak to the necessity to provide limited access to NPSBN resources according to the roles and responsibilities of both NPSBN internal users as well as PSEN users. Access requirements also include limiting the access that a user has to the various PSEN networks connected to the NPSBN by identifying the rights users have to various information types. Following are requirements for access control.

Table 100. Access Control Requirements

#	Requirement
1	The NPSBN SHALL support access controls necessary to limit users from access to network control and signaling assets.
2	The NPSBN SHALL support the ability based on a users identity to limit or expand access to either shared or private services served locally, regionally, or nationwide including other PSENs.
4	The NPSBN SHALL have the ability to shut off access to all or individual network components or network interfaces based on detected illegal or illegitimate activities either by a device or a user.
5	The NPSBN SHALL have the ability to shut off access of rogue or lost devices, or any other device according to policy.

#	Requirement
6	The NPSBN SHALL have the ability to shut off access of a suspended, fired, or illegal user or account, or to any account according to policy.

5.14 Encryption, Certificates, and Keys

The requirements for network encryption, certificates, and keys speak to the necessity to provide the appropriate type of data protection capabilities for NPSBN users and agencies. These network services will allow users and agencies flexible mechanisms to protect data in transit through the use of encryption methods, certificates, and keys. The requirements assure that the NPSBN will both supply and support various transport mechanisms for encryption. FIPS 140-2 encryption standards are presently the required standard for federal agencies and a generally accepted standard for sensitive information by local, tribal, and state agencies. The included requirements are defined in such a way as to support present and future local, tribal, state, and federal agencies requirements for proper data protection. Presently, for federal agencies FIPS 140-2 encryption is mandatory for securing data. Following are requirements for network encryption, certificates, and keys.

Table 101. Encryption, Certificates, and Key Requirements

#	Requirement
1	The NPSBN SHALL provide a Certificate Validation Service and Directory Service for management of keys and certificates to be used by applications and services to enable VPN, MVPN, and other secure communications.
3	The NPSBN SHALL support the transport of standards-based IPsec and other tunnel-based VPN and MVPN technologies without an adverse impact on either the data or the network components.
4	The NPSBN SHALL support the transport of VPN technologies that preserve the necessary data to assure operations of the QoS and Priority Services available on the network.

5.15 Network Signaling and Controls Protection

The requirements for network signaling and controls protection are designed to ensure that the NPSBN infrastructure is protected from the illegal access and/or other threats created by improper protections on infrastructure signaling and control components. Network signaling and controls are the communication packets used in configuring various network components including LTE core components, switches, routers, and servers on the network. Following are requirements for network signaling and controls protection.

Table 102. Network Signaling and Controls Protection Requirements

#	Requirement
1	The NPSBN SHALL protect using encryption and access control the network signaling, configuration, and other control interfaces of the network.
2	The NPSBN SHALL limit access by user, function, and on a need-to-know basis to network control components.
3	The NPSBN SHALL log and monitor all network control and signaling activities, and alerts will be generated when improper activity is detected.
4	The NPSBN SHOULD provide background requirements to be met before granting access to any individual for network control components for either monitoring or configuration purposes.

5.16 External Interfaces and Roaming

The requirements for external interfaces and roaming security are designed to ensure that the NPSBN is properly protected at the interfaces to external entities from threats that may exists at the boundaries. Following are security requirements for external interfaces and roaming.

Table 103. External Interfaces and Roaming Requirements

#	Requirement
1	The NPSBN SHALL consider all independent agency networks as untrusted interfaces unless otherwise certified as trusted zones and agreed upon between agencies.
2	The NPSBN SHALL provide firewall, IDS, and other cyber security protection devices at the interface points where untrusted network interfaces connect to the network.
3	The NPSBN SHALL provide sensor data from the deployed sensor devices to the Security Operations for threat and operational analysis and response.
4	The NPSBN SHALL have the ability to shut down any external interface or connection to roaming network if security threats are detected and determined to be a threat to NPSBN operations.

5.17 UE Security

A variety of UE consumer devices such as smartphones, Personal Computers (PCs), tablet PCs, modems, and customer premise equipment (CPE) in fixed, portable, and vehicular configurations are available today for operation on commercial networks. Public safety expects that equivalent devices, capable of operating both on commercial networks and on the NPSBN, will be available. The NPSBN-U will require devices that provide appropriate security for operating system software, applications, and physical configurations. Following are security requirements for UE devices.

Table 104. UE Security Requirements

#	Requirement
1	NPSBN UE SHALL be compliant with the security requirements of the Network Services, User Service, and Transport sections of this specification.
2	NPSBN-Us SHOULD require UEs that can be completely disabled remotely (i.e., “kill”) when compromised.

5.17.1 Device Management

When UEs are initially configured, an authorized entity will be capable of configuring the security criteria for the UE. The security criteria include local UE access, network access security, transport encryption, payload encryption, and VPN configuration.

Following are security requirements for UE management.

Table 105. Device Management Network Security Requirements

#	Requirement
1	The device management network service SHALL allow an authorized entity to install and enable malware/anti-virus protection.

5.17.2 UE Lockdown

Once UEs are authorized on the network, there will be occasions when the UEs need to be deactivated or disabled. If a UE is lost or damaged, an authorized entity will permanently remove the UE from the network, preventing unauthorized access with the UE. In some cases, the entity will want to perform a full wipe of the UE, removing all installed applications, credentials, and stored files from the UE.

In the event that a UE needs to be temporarily deactivated, such as in the case of a suspended user, the device management network service shall provide a function to temporarily disable local access to the UE, as well as prevent the user or applications from accessing the network. The network should be able to communicate with the UE in order to re-enable, wipe, or disable the UE. Certain functions such as remote microphone or video activation and transport may be available, but they are out of the scope of this section.

The network service shall also provide a mechanism to lock down the UE in the event it appears that an unauthorized access attempt has occurred, such as a certain number of failed login attempts either on the UE itself or to some aspect of the network. Following are requirements for UE lockdown.

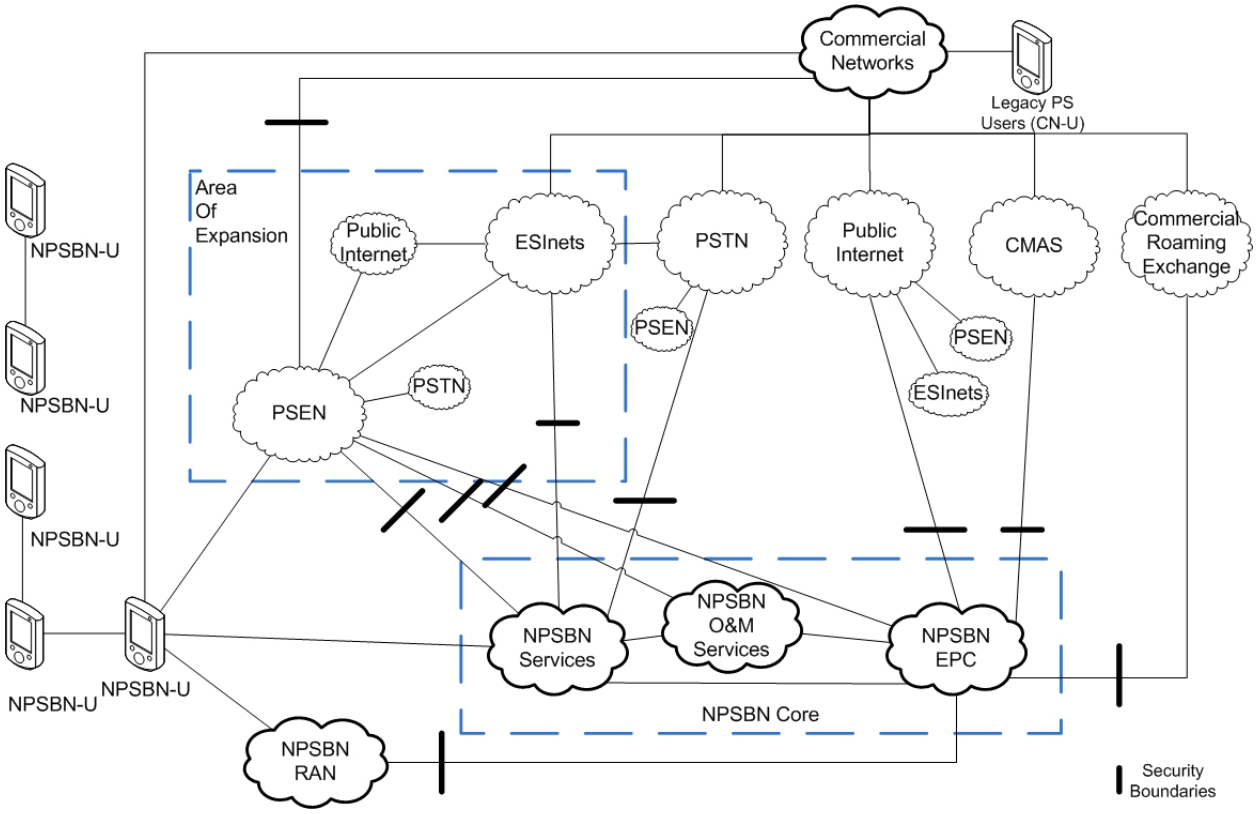
Table 106. UE Lockdown Requirements

#	Requirement
1	The device management network service SHALL allow an authorized entity to remotely perform a full data wipe of a UE on the network.
2	The NPSBN SHALL provide for an authorized entity to permanently remove a UE's ability to access the NPSBN.
3	The device management network service SHALL allow an authorized entity to temporarily remove a UE's ability to access the NPSBN.
4	The NPSBN SHALL provide the ability to lock out NPSBN UEs on commercial carrier networks.

5.18 Transport Security Requirements

This section addresses the security in place to protect the integrity, availability, and confidentiality from a Transport perspective. Users will rely on the NPSBN to provide security of the Transport system to protect their users, their data, and their PSENs. Further, FirstNet will have an obligation as part of that protection to establish minimum connection and Information Assurance criteria such that connecting PSENs have both a minimum standard to strive to and have confidence that their peers who are connected have also met those standards. In more specific terms, Information Assurance can be defined as, from a security perspective, the protection of both the systems and the data traversing or stored on those systems from both internal and external threat, both physical and cyber related. By accepting this obligation, FirstNet will be establishing a level of mutual trust between the PSEN communities. The security boundaries as outlined in Figure 7 will be required to be protected, monitored, and logged.

Figure 7. Security Boundaries



Following are PSEN to NPSBN transport requirements.

Table 107. PSEN to NPSBN Transport Requirements

#	Requirement
1	FirstNet SHALL be responsible for defining a minimum Information Assurance level for PSENs that wish to connect to the NPSBN.
2	FirstNet SHALL use appropriate mechanisms to secure and protect user, management, and control plane traffic.
3	All links between the PSEN and the NPSBN SHALL be properly protected by FirstNet if they traverse insecure domain/area.
4	FirstNet SHALL have the ability to block all traffic originating from or destined for the PSEN not mutually agreed to be sent or received by both FirstNet and the PSEN.

Following are user to NPSBN transport requirements.

Table 108. User to NPSBN Transport Requirements

#	Requirement
1	If the NPSBN provides a VPN capability, that capability SHALL meet industry acceptable encryption levels for the passing of public-safety grade information.
2	The NPSBN VPN capability, if provided, SHALL support VPN clients that are compatible with deployed and supported operating systems.
3	User agencies SHALL be permitted to provide their own VPN solutions for accessing their PSEN.
4	Any data stream, sent or received by the NPSBN-U that only traverses the NPSBN, and is considered sensitive or privileged by local, tribal, state, or federal statute or policy SHALL be encrypted.
5	Any data stream sent or received over commercial or other networks via non-FirstNet devices, that is considered sensitive or privileged by local, tribal, state, or federal statute or policy SHALL be encrypted.

Following are system function to NPSBN transport requirements.

Table 109. System Function to NPSBN Transport Requirements

#	Requirement
1	The NPSBN SHALL encrypt all system control links that cross administrative boundaries (e.g., eNodeB to EPC) to maintain proper Information Assurance at both a user and system level.
2	The NPSBN SHALL implement access controls/firewalls to prohibit unallowed network connections and traffic.
3	The NPSBN SHALL establish procedures for application owners to open required ports and protocols for access control/firewall traversal.
4	The NPSBN SHALL inspect all network traffic at security boundaries for intrusions.
5	The NPSBN SHALL inspect all network traffic as possible based upon encryption level at security boundaries for malware and viruses.
6	The NPSBN SHOULD actively prevent intrusions.

Following are NPSBN transport monitoring requirements.

Table 110. NPSBN Transport Monitoring Requirements

#	Requirement
1	The NPSBN SHALL monitor and log the transport network for security vulnerabilities and

#	Requirement
	violations with the intent of providing improved application, service, and general availability.
2	The NPSBN SHALL maintain a status of network security accessible by PSEN security personnel.
12	Backhaul equipment SHALL be compliant with applicable standards and regulatory mandates.

5.19 Physical Security for Facilities

This section contains requirements on the physical security of NPSBN network equipment and sites. Physical security guidelines may differ between PSEN jurisdictions and federal facilities, therefore the list does not claim to cover every possible facet of known and enforceable physical security policy. Further, how and what security measures can be implemented and who bears the cost of upgrades are yet to be determined.

Following are physical security requirements for NPSBN infrastructure facilities.

Table 111. Physical Security for Facilities Requirements

#	Requirement
1	Physical security of sites SHALL prevent unauthorized access.
2	Local PSEN O&M administrators SHALL be provided with means to monitor alarms in their respective service area.
3	Outdoor radio sites SHALL be equipped with physical and/or electronic means to detect, monitor, and deter unauthorized entry.

Intentionally Blank

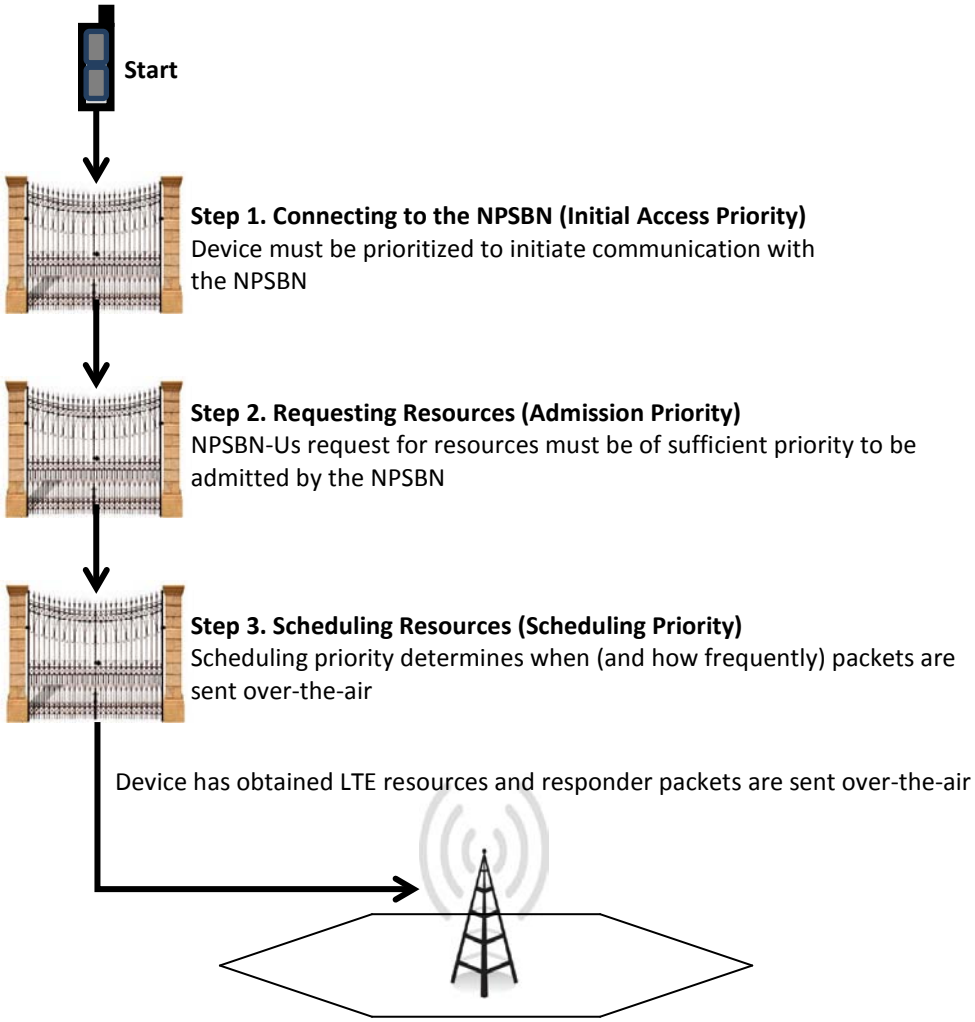
6 Priority and Quality of Service

Prioritization and Quality of Service (QoS) are essential functions in the nationwide public safety broadband network (NPSBN). Prioritization is the network's ability to determine which NPSBN-U resources should be admitted to the NPSBN. Quality of service is the network's ability to ensure that IP packet flows associated with different applications satisfies performance objectives (e.g., packet loss, delay, and throughput) needed for different applications to operate. Thus, prioritization addresses authorization to use NPSBN resources while QoS addresses the treatment of traffic after the resource is established.

Requirements in this section are derived from the NPSTC Priority and QoS Task Group, which captured user needs for Priority and QoS on the NPSBN [4].

Figure 8 outlines the overall process for an NPSBN-U to obtain priority and QoS from the NPSBN.

Figure 8. Priority and QoS Process



Section 6.1.3 defines requirements concerning Step 1 (Initial Access Priority) in Figure 8. The user requirements concerning Step 2 (Admission Priority) are broken into Sections 6.1.4 and 6.1.5. Finally, Section 6.1.2 defines requirements concerning Step 3 (Scheduling Priority).

6.1 Configuring Priority and QoS

Priority and QoS consists of three parts:

- (Quality of Service) Providing sufficient packet transfer characteristics for admitted resources – Section 6.1.2.
- (Access Control) Initial connection by the NPSBN-U to the NPSBN – Section 6.1.3.
- (Admission Priority) Admitting an NPSBN-U's resource request by the NPSBN – Sections 6.1.4 and 6.1.5.

While it is possible for an NPSBN administrator to manually configure each of the aforementioned Priority and QoS attributes, this is cumbersome. The act of configuring and utilizing the NPSBN for Priority and QoS services must be a simple, consistent service for all users of the NPSBN. Following are requirements for priority and QoS configuration in the NPSBN.

Table 112. Priority and QoS Configuration Requirements

#	Requirement
1	When assigning default priority and QoS to an NPSBN-U, the authorized administrator (NPSBN or PSEN)SHALL have the ability to choose from a list of standardized 'templates.'
2	It SHALL be possible for an authorized administrator (NPSBN or PSEN) to alter, in run-time (i.e., while the NPSBN is operating), the template assigned to an NPSBN-U or group of NPSBN-Us.

6.1.1 End-to-End Priority and QoS

To provide consistent end-to-end treatment of public safety traffic, prioritization of NPSBN resources must be provided both over the air as well as within the network infrastructure. Backhaul and IP network priorities need to be aligned to match the priority of over-the-air resources.

The IP transport that is used to carry public safety user traffic between the NPSBN infrastructure elements should be configured in a manner consistent with the assigned Quality of Service (Section 6.1.2) of the NPSBN resource. This means a consistent mapping between NPSBN-assigned scheduling priority and transport/backhaul priority needs to be devised. Further, this mapping must be consistently applied to the entire NPSBN (all territories). This document does not attempt to require a specific mapping of NSPBN priority to the myriad of backhaul and IP technologies available.

Failure to align NPSBN scheduling priority with IP network/backhaul priority will significantly reduce the quality of the end user's experience. For example, voice and video may be choppy (excessive packet loss or delay) or entire sessions may be lost.

Following are requirements for end-to-end priority and QoS in the NPSBN.

Table 113. End-to-End Priority and QoS Requirements

#	Requirement
1	NPSBN backhaul, transport, and IP packet prioritization techniques SHALL be consistently applied to the entire NPSBN.

6.1.2 Quality of Service

Once an NPSBN-U has a resource admitted to the NPSBN (i.e., the admission attributes of Sections 6.1.3and 6.1.4 have been evaluated and the NPSBN has determined that resources should be granted), quality of service scheduling priority attributes determine when and how traffic should be sent to or received from the device. Quality of service is associated with the application being used and not with public safety attributes (like a responder's role). Like admission priority, an authorized administrator typically assigns quality of service.

Scheduling priority considers the following attributes in both the downlink and uplink directions:

- Packet latency
- Packet loss rate

Following are requirements for quality of service in the NPSBN.

Table 114. Quality of Service Requirements

#	Requirement
1	On a per-application flow basis, it SHALL be possible for the NPSBN to assign and control the packet latency and packet loss characteristics.
2	The NPSBN SHALL be capable of determining which application flow a packet is associated with when neither MVPN nor VPN technology is being used.
3	The NPSBN SHALL be capable of determining which application flow a packet is associated with when MVPN or VPN technology is being used.
4	It shall be possible for an authorized NPSBN administrator to define templates (groupings) for combinations of packet loss and packet latency rates.

6.1.3 Access Priority

Various events such as earthquakes, mass casualty incidents, and the like will cause heavy system access, especially when the public safety spectrum is shared with commercial users as part of a public-private partnership. Such events frequently cause a concentration of responders in a given area. This concentration may result in a heavy load at a given cell, and the load may be so severe that a responder's device is prevented from accessing the NPSBN.

While there are an order of magnitude fewer users on the NPSBN than a comparative commercial LTE system (few million versus tens of millions), care must be taken to prioritize initial system access for the NPSBN user community. Following are admission requirements for the NPSBN.

Table 115. Admission Control Requirements

#	Requirement
1	The NPSBN SHALL distinguish between devices from public safety and secondary users during congestion to allow priority access for first responders if needed.
2	The NPSBN SHALL implement mechanisms to manually restrict secondary user devices from making access attempts at the scene of an incident to minimize system performance degradation. This should not affect 9-1-1 calls originated by secondary users.
3	The NPSBN SHALL automatically throttle access for devices from secondary users during cell overload to ensure first responders can get access to the NPSBN. This should not affect 9-1-1 calls originated by secondary users.
4	The NPSBN SHALL provide the ability to manually control access to the NPSBN for different classes of first responders.

6.1.4 Static/Default Admission Priority

Admission Priority is essentially the ability for different devices, applications, and configured policy (i.e., stored rules in the NPSBN infrastructure) to influence whether or not a responder's request for resources should be granted by the NPSBN. The public safety user community has identified two sets of attributes for determining whether or not to grant an NPSBN-U's resource request:

- Static Admission Priority Attributes – defined in this section
- Dynamic Admission Priority Attributes – defined in Section6.1.5.

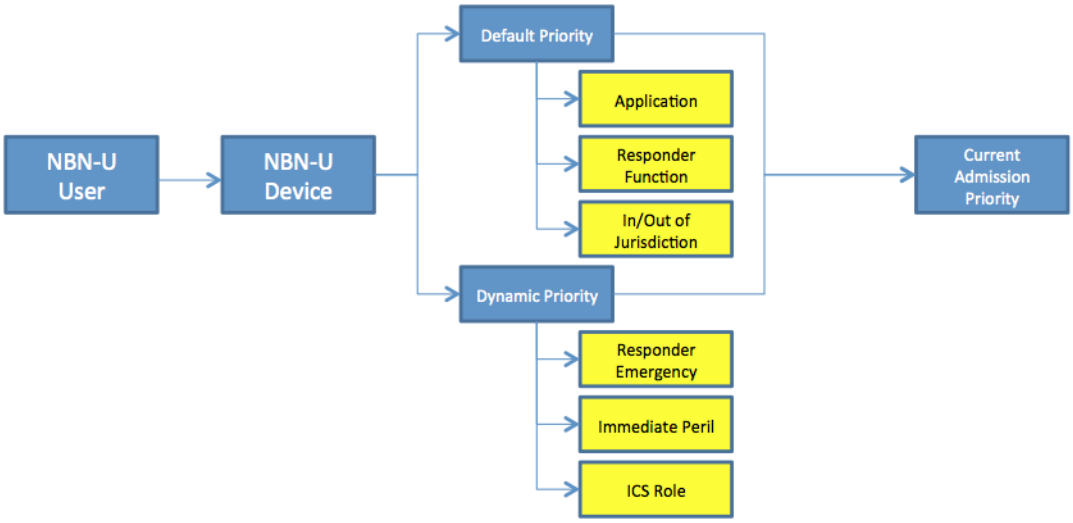
Figure 9 shows the overall role of static and dynamic priority in determining the NPSBN-U's admission priority.

Figure 9. Static and Dynamic Admission Priority

current admission priority = (static priority) + (dynamic priority)

static priority = f(application, responder function, in/out of jurisdiction)

dynamic priority = f(responder emergency, immediate peril, ICS incident role)



Static Admission Priority Attributes can be pre-configured into the NPSBN and do not require human intervention to maintain. In other words, once basic attributes about an NPSBN-U are added to the system, the NPSBN uses these basic attributes to derive the NPSBN-U's default priority when resources are requested from the system. Following are static admission requirements for the NPSBN.

Table 116. Static Admission Priority Requirements

#	Requirement
1	The default admission priority for an NPSBN-U shall be the combination of the Application priority from requirement 3 of this table and the default priority of NPSBN-U, which is based on the user of the NPSBN-U normal role and is set when the NPSBN-U is first configured.
2	The NPSBN SHALL support the following relative application priorities when computing the NPSBN-U's default admission priority (1 = highest relative priority): 1. Mission-Critical Voice 2. Data applications (e.g., CAD, DB queries/RMS, location services, dispatch data, NPSBN-U health/telemetry) 3. Low Priority Voice (e.g., telephony or back-up PTT applications) 4. Video or Multimedia (e.g., streaming, progressive, etc.) 5. Routine text messaging, multimedia messaging, file transfers, device management, web browsing

#	Requirement
	Implementation note 1: The numbers above should not be construed as actual NPSBN configuration values; rather relative rankings compared to the other listed applications. It is further understood that the rankings should be periodically reviewed as new applications become available. Implementation note 2: It is recognized there are multiple methods to realize text messaging (e.g., control channel, over-the-top, etc.) and the ability of LTE technology to satisfy this requirement varies with the method selected.

6.1.5 Dynamic Priority and QoS Control

By nature, public safety operations are situational. It is impossible to statically pre-configure a single set of priority and Quality of Service (QoS) values for a responder to address all operational needs. The nature of the responder's current situation, incident, and role ultimately influences their priority and QoS. Dynamic priority and QoS control is a service provided by the NPSBN to authorized end-responders and administrators to override default day-to-day priority and QoS provided to a responder. Simply stated, dynamic priority and QoS allows responders to obtain resources during periods of heavy NPSBN congestion, subject to a nationally-approved framework.

Admission priority concerns the ability for different devices, applications, and configured policy to influence whether or not a responder's resource request should be granted by the NPSBN. Section 6.1.4defines the static attributes (e.g., type of application) that are used to influence admission priority. This section identifies the dynamic public safety attributes that also influence admission priority.

Following are general requirements for dynamic priority and QoS.

Table 117. Dynamic Priority and QoS General Requirements

#	Requirement
1	The NPSBN SHALL provide a 'Dynamic Priority and QOS control service' to allow suitable PSEN and mobile applications to override the default day-to-day priority assigned by the PSEN administrator.
2	NPSBN LTE users and Non-LTE public safety users SHALL NOT be burdened by the NPSBN with priority and QoS control outside of their operational paradigms. It is understood that human intervention is required to initiate a dynamic Priority and QoS change, but the act of performing this change should not significantly distract the responder. For example, the responder should be able to press an emergency button for a life-threatening condition and not have to enter an LTE terminal to adjust complex LTE priority and QoS parameters.

#	Requirement
3	The NPSBN SHALL provide an interface to each PSEN in order for PSE applications to invoke dynamic Priority and QoS changes for the PSE's associated NPSBN-Us. The intent is to say triggering Priority and QoS changes should be integrated into the responder's existing applications and workflow.
4	The NPSBN SHALL provide a profile (documented configuration standards) to all entities using Priority and QoS. This profile will ensure consistent treatment of NPSBN-U resources across the entire NPSBN.
5	The NPSBN SHALL provide usage records to individual agencies, identifying usage of dynamic priority and QoS controls described in this section. The intent of this requirement is for the NPSBN to supply usage or billing records. The intent is for supervisors to be able to identify usage patterns of dynamic priority and QoS usage by specific NPSBN-Us.
6	The NPSBN SHALL provide near-real-time usage alerts to the PSEN and the initiating NPSBN-U's associated device(s) when any dynamic priority and QoS control described in this section has been activated or de-activated. The intent of this requirement is to provide notification to PSEN administrators and the NPSBN-U device that one or more of their NPSBN-Us are currently in a heightened usage state.
7	NPSBN-Us operating on the NPSBN, when attempting to communicate with devices operating on other networks, SHOULD be able to convey end-to-end priority needs to the interconnected IP-based system(s) in order to increase the probability of completing communications during periods of network congestion or impairment. Responders often need to interact with the public in the same area of an incident. Congestion in either the NPSBN or external (e.g., commercial) system can result in a lowered probability of call success. This requirement will likely have impact to interconnected systems (e.g., commercial carriers).
8	When an NPSBN-U receives an incoming call from a non-public safety system (e.g., peer IP-based systems such as the Internet and commercial networks), it SHOULD be possible for the originating IP-based system to convey end to end priority needs to the NPSBN in order to increase the probability of completing communications during periods of network congestion or impairment.
9	It SHALL be possible for an authorized NPSBN-U to view in near real-time the current priority and QoS settings for themselves or for another NPSBN-U from the same PSE. The intent, for example, is for a responder or dispatcher to be able to see that a dynamic priority and QoS setting has been activated for a particular user.

Dynamic Priority and QoS on the NPSBN is controlled by three factors:

- **Responder Emergency** – an indication from an end-responder or administrator that a responder is in a life-threatening situation – Section 4.2.2.
- **Immediate Peril** – an indication from an end-responder or administrator of an immediate threat to human life – Section 4.2.3.
- **ICS Incident Priority**– Defining the linkage of assigned incident type and role from the Incident Command System to NPSBN Priority and QoS – Section 4.2.4.

It should be emphasized that these dynamic controls can be utilized simultaneously for a given user.

6.2 Pre-emption

Pre-emption refers to the immediate removal of a NPSBN-U's resources, often without warning to the NPSBN-U. As of this writing, U.S. public carriers do not support pre-emption for devices roaming onto their system. Most LMR system operators also avoid pre-emption today. Instead, talkgroups are prioritized and, at worst, responders experience an increased queuing delay during system access.

The environment of the NPSBN is different than LMR systems. Unlike LMR, all NPSBN applications share a single set of resources. This means high-bandwidth video applications and mission critical voice share a common set of resources. Certain responder situations (e.g., responder emergency) require the ability to instantly obtain resources for mission critical service. Following are requirements for pre-emption in the NPSBN.

Table 118. Pre-emption Requirements

#	Requirement
1	The NPSBN SHALL support the ability to instantly remove resources from one NPSBN-U application and make those resources available to another NPSBN-U application.
2	It SHALL be possible for an authorized NPSBN administrator (NPSBN and PSEN) to configure which applications can utilize resources previously assigned to other applications.
3	The NPSBN SHALL support the ability to change whether or not a given application can be pre-empted, based on triggers from an application or NPSBN-U.

The reader is encouraged to reference these additional pre-emption requirements in other portions of this document:

- Table 40. Responder Emergency Requirements
- Table 119. Priority and QoS for Secondary User Requirements

6.3 Secondary Users

The legislation [1] supports the possibility of FirstNet engaging in public-private arrangements to construct, manage, and operate the NSPBN. This provides for the possibility of secondary use of the

NPSBN spectrum by secondary users. At a minimum, secondary users are non-public safety users. Because of the possibility of the existence of secondary users, this section attempts to clarify the Priority and QoS relationship between primary and secondary users of the NPSBN spectrum. Following are requirements for priority and QoS for secondary users in the NPSBN.

Table 119. Priority and QoS for Secondary User Requirements

#	Requirement
1	Secondary users SHALL be able to access the NSPBN so long as the act of connecting to the NPSBN does not in any way interfere with or prevent a primary user from accessing the NSPBN. See Section 6.1.3.
2	Secondary users SHALL be able to obtain resources from the NPSBN so long as the act of obtaining resources from the NPSBN does not in any way pre-empt resources previously obtained by a primary user or prevent a primary user from obtaining resources. See Section 6.1.4.
3	When a primary user attempts to obtain resources and congestion is present, the NPSBN SHALL pre-empt secondary user resources in order to admit the primary user's resource request. The intention is to pre-empt high bandwidth applications first, such as streaming multimedia services, before pre-empting voice services.
4	Should pre-emption be required, the NPSBN SHALL first pre-empt secondary user resources before pre-empting any resources used by a primary user.

6.3.1.1 General QoS Management Requirements

Following are general O&M requirements for QoS management.

Table 120. General O&M QoS Management Requirements

#	Requirement
1	The NPSBN SHALL provide a means for PSE O&M authorized users to configure the default priority (as defined in Table 6, Requirement #2) and QoS settings of users within their scope.
2	The NPSBN SHOULD provide an O&M tool to provide the QoS management capabilities described herein (see also Section 6.1.5).

6.3.1.2 QoS Configuration Requirements

The requirements of Table 121 and Table 122 describe PSE O&M users needs to configure QoS capabilities and view an historical log of changes. Following are requirements for QoS configuration.

Table 121. QoS Configuration Requirements

#	Requirement
1	The QoS configuration capability SHALL allow suitably authorized public safety O&M users to define/assign QoS roles for their PSE.

Public safety has a need to track changes to important operational parameters so that ongoing and post-event analysis can identify the causes and corrective actions of communications problems. Following are requirements for QoS configuration history.

Table 122. QoS Configuration History Requirements

#	Requirement
1	Suitably authorized PSE administrators SHALL be able to view a QoS configuration history for users under their authority.
2	Suitably authorized PSE customer service representatives SHALL be able to view a QoS configuration history for users under their authority.

6.3.1.3 Priority and QoS Monitoring Requirements

Table 123 identifies requirements pursuant to the needs of public safety network management personnel to monitor the QoS of users within their jurisdiction and organization.

Table 123. QoS Monitoring Requirements

#	Requirement
1	PSE network managers SHALL be able to view the real-time dynamic priority condition of all users under their authority.
2	PSE network managers SHALL be able to retrieve information that allows for “post-mortem” evaluation of the effectiveness of QoS configurations in providing for effective incident communications.

6.3.1.4 QoS Control Requirements for O&M Users

In the confusion of incidents and emergency events, it is sometimes the case that operational personnel, such as dispatchers, being focused on mission, are less than diligent in “cleaning up“ afterwards. Historically, public safety has relied on O&M users to be able to restore the normal operating priorities of their systems following such events. Following are O&M user requirements for QoS control.

Table 124. QoS Control by O&M Users Requirements

#	Requirement
1	PSE network managers SHALL be able to modify the QoS role of users within their scope.

7 Conclusions and Recommendations

The overall purpose of this document is to provide preliminary high-level technical and administrative requirements potentially applicable to the planned deployment and operation of FirstNet's NPSBN for consideration by FirstNet.

The three main conclusions and recommendations are:

- FirstNet should consider the high-level launch requirements defined by NPSTC while deploying and operating the NPSBN.
- Further efforts are required to define more detailed requirements based on those defined in this document for use in accelerating the deployment and operation of the NPSBN. Related requirements may be needed to support the development of RFPs, etc. in this regard.
- NPSTC encourages FirstNet to engage with NPSTC on how the high-level launch requirements defined in this document can be further articulated to promote the accomplishment of relevant legislation that supports the establishment of a nationwide public safety broadband network that meets the current and emerging needs of the public safety community.

7.1 Best Practices

For a task of this magnitude a fragmented approach based on each jurisdiction's best intentions will result in a sub-optimal outcome – the "bottom-up" method of systems design will not work. Nationwide standards need to be developed and embraced by local, tribal, state, and federal jurisdictions. The public safety community would recommend that we all start working toward standards and best practices that will simplify and unify operations and ultimately reduce overall O&M costs. Once defined, these standards will allow a consistent structure within which the adopters can deploy and operate.

7.1.1 Standards for Procurement

Two of the greatest obstacles during the build out of the NPSBN will be cost and compatibility across the system. To ensure these two needs are met, it is critical that standardization begin at the procurement phase. It is recommended that a template for procurement be developed and that the template package be completed prior to deployment. At a minimum any operator, maintainer, or end users will only be able to procure equipment that is authorized and approved by FirstNet or is in the approval process. The procurement process shall follow best practices for procurement in the public sector.

7.1.2 Standards for Construction to Public SafetyGrade

To ensure all systems are built to the same standard, it is highly recommended that a clearly defined minimum set of standards be adopted to define "public safety grade" for the Network. There are many components that must be addressed such as coverage calculations, tower construction, equipment installation, environmental controls, and many other requirements. It is therefore recommended that a

list of standards be adopted and followed. Some standards already exist for many of these components, and should be used as a baseline for the development of a defined "public safety grade."

Standards for Coverage

The level of coverage needed or necessary in all areas will be developed and agreed upon by local, county, state, tribal and federal entities and their needs will be considered on a case by case basis, e.g., population considerations, level of protection needed for all areas. Adoption rates will greatly influence the utility of the network in any particular area and drive the costs to build and maintain. Having pervasive coverage will optimize the usefulness of the network, but the overall costs may be prohibitive under some circumstances. A minimum level of coverage standard or a graduated set of standards would help the dialogue between FirstNet and the states.

Who will pay and how is a consideration. The legislation is written to provide ample opportunities to be creative when considering the development of public/private partnerships. Such partnerships will be especially instrumental in obtaining adequate coverage and paying for installation and maintenance of the system in underserved, rural areas.

One of the most difficult tasks in building a communication system is accurate coverage prediction, which is made even more difficult with LTE where coverage and capacity are directly coupled. It is recommended that a single coverage/capacity model is adopted that provides accurate and validated predictions within the NPSBN spectrum.

7.1.3 Standards for Operation

Every effort should be made to prevent a fragmented approach from complicating the NPSBN. The network, interfaces, and protocol standards that have been created for LTE must be clarified to ensure all systems are compatible from day one.

In addition, to assure high levels of excellence, interoperability, repeatability and uniformity; consistent Standard Operating Procedures for day-to-day usage will need to developed on a nation-wide basis.

7.1.4 Standards for Training and Exercises

Training standards for user classes/types should be developed to address specific user needs and capabilities. All public safety personnel will need initial and ongoing training to assure a thorough understanding and an instantaneous, reflexive ability to utilize the new tools to be delivered via the NPSBN. Additionally, communications and administrative personnel will need specialized training as many of the services and applications inherent to FirstNet will interface directly with communications centers. In many cases, IP network administration, operations, and management training will be required. As always, hands on training through exercises will be needed to truly understand and optimize newly acquired tools and tactics in delivering the public safety value proposition.

7.1.5 Standards for Governance

As with any connected system, there must be a governance body composed of stakeholders; however, all too often the governance body is an afterthought. At a minimum any entity accepting federal grant money shall be bound by a joint powers agreement or other instruments that requires shared use of the system.

- **User Setup and Provisioning**: One of the key functions required of FirstNet will be to establish a uniform and streamlined setup process to add new participants and devices to the network by the local, tribal, state, and federal entities (jurisdictions) and well as any potential secondary users. Such processes will also include the ability to change and remove participants and devices. From a day-to-day perspective, such actions will be the most common interface between FirstNet and the jurisdictions; thus, policies establishing consistent user setup procedures will need to be developed by FirstNet in collaboration with the public safety community to assure interoperability across jurisdictions and during deployment to remote jurisdictions.
- **Fee Management:** The initial setup will also trigger the Fee Management function where charges to a jurisdiction will be tied to the participant or device. Thus, the interaction between local, tribal, state, and federal jurisdictions for the Fee payment options will need to be defined while working with FirstNet (i.e., the states may manage the local and tribal payment process and then pay FirstNet one lump sum or FirstNet may manage the payment process down to the local jurisdiction level.)
- **Help Desk Function**: In addition to the Setup and Fee Management functions, the HelpDesk function for the reporting of network problems will be another function provided by FirstNet. The boundary line between nationwide network and state and local support for trouble-shooting must be clearly defined.
- **Service-Level Agreements**: Finally, as part of the RAN requirements discussion and also related to the HelpDesk function, there must be Service Level Agreements (SLA) that clearly define all aspects of roles and responsibilities related to the network and the RAN, including turn-around times for repair/replacement and who will respond to problem calls and what those costs will be.
- **Tribal Control**: Tribes have a government-to-government relationship with the United States with certain established responsibilities, powers, limitations and obligations attached to that relationship. Therefore, in consultations with these federally recognized tribes, FirstNet must acknowledge and consider existing issues of tribal sovereignty and federal trust principles in the development of the NPBSN.

Although truly mundane in nature, it is these day-to-day “back-office” tasks that can make or break the perception of an operational system as being “the best” or “the worst.”

Intentionally Blank

8 References

[1] "Middle Class Tax Relief and Job Creation Act of 2012," (PL 112-96, 22 Feb. 2012). Title VI—Public Safety Communications and Electromagnetic Spectrum Auctions. 126 Stat. 201: §6001–6703. Codified: 47 U.S.C. §1401. Available: http://www.gpo.gov/fdsys/pkg/PLAW-112publ96/pdf/PLAW-112publ96.pdf. Cited September 2012.

[2] "Communications Act of 1934," (PL 416, 19 Jun. 1934). Title 47—Telegraphs, Telephone, and Radiotelegraphs. 48 Stat. 1064: §337(f). Codified: 47 U.S.C. §337(f). Available: http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/pdf/USCODE-2011-title47-chap5-subchapIII-partI-sec337.pdf. Cited September 2012.

[3] "Homeland Security Act of 2002," (PL 107-296, 25 Nov. 2002). Title 6—Domestic Security. 116 Stat. 2135: §101. Codified: 6 U.S.C. §101. Available: http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf. Cited September 2012.

[4] Broadband Working Group – Priority and Quality of Service Task Group, NPSTC, "Priority and QoS in the Nationwide Public Safety Broadband Network," Rev 1.0, April 17, 2012. Available: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2304&file=PriorityAndQoSDefinition_v1_0_clean.pdf. Cited September 2012.

[5] Broadband Task Force, NPSTC, "700 MHz Public Safety Broadband Task Force Report and Recommendations," September 4, 2009. Available: http://www.npstc.org/download.jsp?tableId=37&column=217&id=10&file=700_MHz_BBTF_Final_Report_0090904_v1_1.pdf. Cited September 2012.

[6] Federal Communications Commission, "In the Matter of the Commercial Mobile Alert System." First Report and Order, FCC 08-99 (PS Docket No. 07-287, 9 Apr. 2008). Available: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-99A1.pdf. Cited September 2012.

Second Report and Order and Notice of Proposed Rulemaking, FCC 08-164 (PS Docket No. 07-287, 8 Jul. 2008). Available: http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-08-164A1.pdf. Cited September 2012.

Third Report and Order, FCC 08-184 (PS Docket No. 07-287, 7 Aug. 2008). Available: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-184A1.pdf. Cited September 2012.

See also Federal Communications Commission, "Commercial Mobile Alert System (CMAS)." Available: http://www.fcc.gov/cgb/consumerfacts/cmas.html. Cited September 2012.

[7] Public Safety MMES Working Group, NPSTC, "Use Cases & Requirements for Public Safety Multimedia Emergency Services (MMES)," Rev B, May 2012. Available: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2354&file=Use_Cases_Rqmts_PS_MMES_Report_120531.doc. Cited September 2012.

[8] AFST Working Group, NPSTC, "Public Safety Communications Assessment 2012 – 2022 — Technology, Operations, & Spectrum Roadmap," Final Report, June 5, 2012. Available:

http://www.npstc.org/download.jsp?tableId=37&column=217&id=2446&file=AFST_NPSTC_Report_06232012.pdf. Cited September 2012.

[9] OMB, Memorandum M-08-23, "Securing the Federal Government's Domain Name System Infrastructure," August 22, 2008. Available: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf. Cited September 2012.

[10] Wikipedia, "Service Delivery Framework," July 27, 2011. Available: http://en.wikipedia.org/wiki/Service_delivery_framework. Cited September 2012.

[11] Telemanagement Forum, "Software Enabled Services Management," July 2012. Available: http://www.tmforum.org/SoftwareEnabledServices/4664/home.html. Cited September 2012.

[12] XML Protocol Working Group, Web Services Activity, W3C, "SOAP Version 1.2," Version 1.2, March 2007. Available: http://www.w3.org/2000/xp/Group/. Cited September 2012.[13] GSM Association, OneAPI. Available: http://Oneapi.gsma.com. Cited September 2012.

[14] NIST, NIST Special Publication 800-63-1, "Electronic Authentication Guideline," December 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf. Cited September 2012.

[15] OMB, Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003. Available: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf. Cited September 2012.

[16] Broadband Working Group, NPSTC, "Local Control in the Nationwide Public Safety Broadband Network," Revision F, March 2012. Available: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2254&file=LC21 Local Control Definition Rev F.pdf. Cited September 2012.

[17] 47 CFR Part 90 Subpart N, "Operating Requirements," 90.423 a) 3, October 2010. Available: http://www.gpo.gov/fdsys/pkg/CFR-2010-title47-vol5/pdf/CFR-2010-title47-vol5-sec90-423.pdf. Cited September 2012.

[18] 47 CFR Part 12, "Redundancy of Communications Systems," October 2010. Available: http://www.gpo.gov/fdsys/pkg/CFR-2009-title47-vol1/pdf/CFR-2009-title47-vol1-part12.pdf. Cited September 2012.

[19] CCITT X.800, International Telecommunications Union (ITU), "Security Architecture for Open Systems Interconnection for CCITT Applications," Geneva Switzerland, 1991. Available: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.800-199103-I!!PDF-E&type=items. Cited September 2012.

Appendix A Acronyms and Abbreviations

This section provides a list of the acronyms and abbreviations used in the document.

3GPP	3rd Generation Partnership Project
AC	Admission Control
API	Application Program Interface
ARP	Allocation and Retention Priority
BBWG	Broadband Working Group (NPSTC)
BIA	Bureau of Indian Affairs
CAD	Computer Aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CJIS	Criminal Justice Information Services
CMAS	Commercial Mobile Alert System
CN-U	Carrier Network User
CODEC	enCoder/Decoder
CPE	Customer Premise Equipment
DHS	U.S. Department of Homeland Security
E9-1-1	Enhanced 9-1-1
Early Builder	A member of the Early Builders Advisory Council (formerly known as “the waiver recipients”) who comprised the Public Safety Spectrum Trust Operator’s Advisory Committee.
eMBMS	evolved Multimedia Broadcast Multicast Service

EMS	Emergency Medical Services
EPC	Evolved Packet Core
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FirstNet	First Responder Network Authority
GBR	Guaranteed Bit Rate
GETS	Government Emergency Telecommunications Service
GoS	Grade of Service
GPS	Global Positioning System
GSA	General Services Administration
IAFIS	Integrated Automated Fingerprint Identification System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
LMR	Land Mobile Radio
LTE	Long-Term Evolution
MBR	Maximum Bit Rate

MIMO	Multiple-Input and Multiple-Output
MMS	Multimedia Messaging Service
MVPN	Mobile Virtual Private Network
NAT	Network Address Translation
NCIC	National Crime Information Center
NENA	National Emergency Number Association
NFIRS	National Fire Incident Reporting System
NFPA	National Fire Protection Association
NG9-1-1	Next-Generation 9-1-1
NGN-PS	Next-Generation Network – Priority Services
NLETS	National Law Enforcement Telecommunications System
NOC	Network Operations Center
NPSBN	Nationwide Public Safety Broadband Network (FirstNet)
NPSBN-U	NationwidePublic Safety Broadband Network User
NPSTC	National Public Safety Telecommunications Council
O&M	Operations and Maintenance
PC	Personal Computer
PSAP	Public Safety Answering Point
PS	Public Safety
PSE	Public Safety Entity –synonymous with a public safety agency responsible for O&M

PSEN	Public Safety Enterprise Network
PSG	Public Safety Grade
PSST OAC	Public Safety Spectrum Trust Operator's Advisory Council
PSTN	Public Switched Telephone Network
PTT	Push-to-Talk
QCI	Quality of Service Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RFP	Request for Proposal
SIEC	Statewide Interoperable Executive Committee
SIGB	Statewide Interoperability Governing Board
SLA	Service Level Agreement
SMS	Short Message Service
SoR	Statement of Requirements
UASI	Urban Area Security Initiative
UE	User Equipment
USB	Universal Serial Bus
USB-IF	Universal Serial Bus – Implementers Forum
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

WPS	Wireless Priority Service