State of Minnesota

Launch Requirements
For Minnesota Public Safety Broadband Network

Minnesota and FirstNet Consultation Project (MnFCP)
MN-SWIFT 70680

Jackie Mines, Director, Emergency Communication Networks

September 25, 2015

445 Minnesota Street
Suite 137
Saint Paul, Minnesota 55101-5137

O: (651) 201-7550
Email: Jackie.Mines@state.mn.us

Table of Contents

Table of Figures

Table of Tables

Executive Summary

Introduction

On July 10, 2008, Apple launched the Apple App Store.

The Apple App Store allowed Apple to control the quality of applications provided to its end-user customers, owners of iPhones. The App Store permits Apple to serve as gatekeeper to an end-to-end ecosystem and ensures its customers have access to an endless array of applications, developed by tens of thousands of independent software and video game developers, all of which have passed a minimum level of quality assurance and technical review by Apple.

Competitors soon entered the market with similar devices and services, “app” became a household term, and life for the modern consumer would never be the same.

The introduction of the Nationwide Public Safety Broadband Network (NPSBN) provides the public safety community in Minnesota with an opportunity to transform life-saving communications in a similar manner to how consumer applications have changed everyday life. Certainly, public safety uses wireless data today; wherever affordable, it is rare to see a police vehicle without a cellular router and a computer connected to the local Computer Aided Dispatch (CAD), for instance. Today’s cellular services, where and when available, serve first responders very well and meet many day-to-day needs for efficiency and overall situational awareness.

However, public safety cannot count on commercial cellular networks the way they depend on their mission critical radios. During major incidents—such as weather events, natural disasters, structural collapse, acts of terrorism or even power outages—commercial networks are not reliable. They are not reliable because they are not built to withstand major surges in traffic or major incidents; they are built to meet the needs of consumers, and are not architected to public safety grade reliability.

The NPSBN must provide public safety with a highly-reliable, mission-critical network that first responders can depend on for the most serious emergency incidents. It must additionally provide public safety with exclusive access to dedicated wireless spectrum on a network that can withstand natural disasters and for which public safety does not have to compete for access to the network. Furthermore, the NPSBN introduces a new ecosystem for public safety communications. Consumers certainly used mobile data applications prior to July 10, 2008, but with the launch of App Store, they would never again use them the same way again.

First responders use cellular data today, but with the NPSBN—they won’t use it in the same way. The statement of requirements (SOR) as detailed within this report represent the needs of the Minnesota public safety stakeholder community to facilitate their adoption of NPSBN service. They were developed with the support of a broad base of practitioners and subject-matter experts from across the state and cover topics ranging from device form factor to information security and system architecture. These requirements are largely based on work originally performed by the National Public Safety Telecommunications Council (NPSTC), and can be considered a Minnesota annex to the requirements set forth by NPSTC.

The overriding intention of this study is to provide the system provider—be it FirstNet, the state of Minnesota, its vendor or some other entity—a clear description of the State’s needs and requirements as communicated by its stakeholders. Should the system provider meet these requirements, the stakeholders feel confident that the service will be fully successful and achieve long-term sustainability.

Document Purpose

This document contains the state of Minnesota's requirements for adoption of NPSBN service. These requirements are not the requirements of *the state of Minnesota*, as a legal governmental entity, but rather the requirements of *public safety agencies throughout Minnesota*. These requirements were developed by a collaborative group of 43 public safety experts representing all levels of government and all disciplines. Firefighters, law enforcement, paramedics, elected sheriffs, telecommunications technicians, engineers, and volunteers from state, federal, county, local and tribal government as well as the private sector from every corner of the state, representing many hundreds of volunteer hours of effort, are all represented within this set of requirements. We can confidently present these requirements as comprehensive, based on best-practices, and strongly representative of stakeholder needs throughout the state.

These requirements are agnostic; they do not prefer any particular implementation approach or vendor technology. They focus strongly on the "What"—that is, *what the requirement is*, and not the "How"—that is, *how the requirement is satisfied*. These requirements were developed such that they could be relied upon just as easily to review FirstNet's proposal to the state as they could be to form the basis of a state request for proposals for development of stand-alone network.

Document Scope

These requirements are targeted towards the **launch window** for NPSBN services. "Launch window" means a period at and immediately following the launch of FirstNet services. These requirements do **not** represent the State's long-term expectations for FirstNet service. The long-term requirements deemed out-of-scope for this document include fundamental mission-critical features, one-to-many push-to-talk voice services, which are not part of present FirstNet planning priorities.

For detail on the state's long-term expectations, see section *Deployment and Enablement*, pg. 6.

About MnFCP

The primary mission of Emergency Communications Network's (ECN) Public Safety Wireless Broadband Program is to facilitate the implementation of a stand-alone, mission-critical public safety Long Term Evolution (LTE) 4G broadband network to first responders in Minnesota. The Minnesota-FirstNet Consultation Project (MnFCP) is designed to deliver on that goal to Minnesota's First Responders while fulfilling the State's obligations under the 2012 Middle Class Tax Relief and Job Creation Act and the 2013 State and Local Implementation Grant Program.

More information about this project and the state's broadband program is available at:
https://dps.mn.gov/divisions/ecn/Pages/broadband.aspx

Contact

Jackie Mines, Director, Emergency Communication Networks
jackie.mines@state.mn.us
(651) 201-7550

METHODOLOGY

Philosophy

The state of Minnesota MnFCP project team facilitated structured workgroups according to three central tenants; (1) a strong focus on network launch, (2) a strong focus on minimum requirements to support adoption, and (3) an assumption that "mission critical" and "public safety grade" service are realized over the long, and not immediate term.

The goal of the workgroups is to identify the **minimum improvement** over commercial service that would drive the user to adopt FirstNet service, and not the **maximum potential** of the network that will be experienced over the long term. For example, while there is an underlying assumption that eventually, the network will provide ubiquitous coverage at a public safety grade, there is no assumption that the network will provide this degree of service at or near launch; the goal of the workgroup, accordingly, is to define the level of coverage, and service, which would be sufficient to foster adoption of NPSBN services in the state in favor of a commercial alternative.

Workgroup Composition

As detailed in Table 1, ECN commissioned four working subject matter-specific workgroups to support the State's development of requirements before FirstNet. These workgroups are staffed by volunteers that represent a variety of interests, disciplines, and agency affiliations.

Table 1: Workgroup Descriptions

Workgroup	Scope
Applications and NG911	Network services provided to users, Public Safety Emergency Networks (PSENs) and Public Safety Answering Points (PSAPs) including services with an Application Programming Interface (API) accessible over the network and end-user applications including those residing on the NPSBN and on the PSEN. "End-user application" and "network service" includes 911 and NG911.
Devices	End-user devices such as mobile routers, smartphones and terminals.
System and Security	System architecture and information security requirements and PSEN-to-NPSBN interconnection requirements.
Coverage	Wireless coverage of the NPSBN including Radio Access Network (RAN) deployed by FirstNet or by agencies in Minnesota. Includes the NPSBN on BC14 as well as roaming partner(s).

Alignment with the NPSTC Statement of Requirements (SOR)

The work performed in Minnesota was highly aligned with foundational work performed by the National Public Safety Telecommunications Council (NPSTC), and its 2012 "Statement of Requirements: High-

Level Launch Requirements, Statement of Requirements for FirstNet Consideration".[1] Minnesota considers the requirements in NPSTC's SOR as representative of the public safety community as a whole and a *de facto* standard for public safety nationwide. The intent of using the SOR as a basis for Minnesota's requirements was to ensure the highest degree of standardization in requirements development.

Largely, Minnesota's requirements do not deviate strongly from those published by NPSTC. The majority of NPSTC's requirements were endorsed by Minnesota's volunteer review committee. Therefore, the key areas of interest in this requirements document are (1) where, specifically, Minnesota's requirements either deviate from NPSTC's requirements, and (2) where Minnesota has introduced additional requirements.

Directives

Each of the State's requirements includes one of four directives: **shall, shall not, should, and should not**. We intentionally used the same directives used in NPSTC's SOR to ensure our requirements are easily compared to those of NPSTC. Our workgroups interpreted these imperatives as follows:

Table 2: MnFCP Requirements Directives

Directive	Description
SHALL	Features or qualities that are *required* of the service. A service *must* provide these features or will have low-to-no adoption in Minnesota.
SHOULD	Features or qualities that are *desired* of the service. These are value-added features that will substantially improve adoption rates of the service.
SHOULD NOT	Features or qualities that are strongly *not desired* of the service. These are qualities that will substantially reduce adoption rates of the service.
SHALL NOT	Features or qualities that are *refused* by stakeholders in Minnesota. A service with one or several of these features is likely to have low to no adoption in Minnesota.

Baseline Assumptions

The workgroup sessions were conducted with respect to a number of baseline assumptions. In developing requirements with the workgroups, they were encouraged to consider these assumptions as given facts, and to build their needs and wants around these assumptions. These assumptions are as follows:

[1] Available at: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2609&file=BBWG_SoR_Launch_12112012.pdf

Assumption 1: NPSBN (FirstNet) service will be priced competitively with commercial carrier service.

While FirstNet has not published a cost structure at the time of the writing this report, and the state does not have sufficient information to build a cost structure around an opt-out model, the workgroup members assumed that NPSBN service would be competitive priced with commercial carrier services. The workgroups were instructed to consider the term “competitively” as a subjective term. For example, the service may be similarly priced with commercial carrier service, or may be slightly more expensive based on a justifiably higher level of service via the NPSBN. The workgroup did not assume that the service would be considerably more expensive than a commercial carrier alternative; i.e., a premium service for a premium price.

Assumption 2: Long-term, NPSBN service will be as or more reliable than your radio

The workgroups assumed that the NPSBN is, ultimately, intended to be a mission-critical network. Accordingly, any requirements related to coverage, availability of the network, response to issues, and other salient factors were established with the assumption that the NPSBN will provide a public safety-grade level of reliability.

Assumption 3: At launch, NPSB service will not replace your radio

Workgroup members were encouraged to develop their requirements assuming they were not replacing their radios in the near term and would not be during the launch window. Therefore, any requirements related to a push-to-talk service were generally considered value-added features, and not core features that would significantly drive adoption. Compared to other states, this is particularly important in Minnesota, where the vast majority of first responders rely on the statewide ARMER network for their primary radio communications;[2] due to the success of the ARMER program, there is simply not an immediate need for a mission-critical, interoperable, push-to-talk voice solution throughout the state.

Process

In identifying user requirements for FirstNet, the State is leveraging its interoperable communications governance structure to ensure that all key stakeholders have a fair voice in developing and endorsing the final set of requirements. The State’s process for developing and seeking approval for requirements is illustrated in Figure 1 and elaborated upon below.

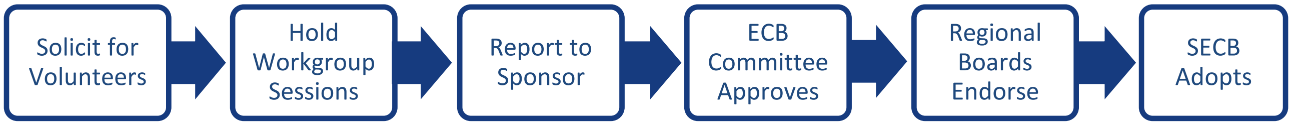


Figure 1: Requirements Development and Approval Process

To ensure maximum consistency with existing requirements sets, we modeled our requirements development off of the National Public Safety Telecommunications Council (NPSTC) *Public Safety*

[2] See https://dps.mn.gov/divisions/ecn/programs/armer/Documents/armer-participation-map-january-twenty-fifteen.pdf. All cities of first-class, state agencies and all but two counties either currently have their primary radio communications on the ARMER system or are in the middle of migrating to ARMER.

Broadband High-Level Launch Requirements Statement of Requirements for FirstNet Consideration (SOR).[3] The requirements enumerated in the SOR were used as a prototype for Minnesota. Workgroup members evaluated each of these requirements on their own merit and determined whether the group agreed with each requirement, disagreed with it, or needed to alter or amend the requirement. The groups also added any new requirements where the SOR did not cover a need either specific to Minnesota, or was simply not included in the SOR. Those areas where Minnesota deviates from the SOR are key interest areas for FirstNet, for the governor's team evaluating FirstNet's proposal, and potentially for any vendor responding to a Minnesota Request for Proposal to implement an opt-out network.

Each workgroup underwent a feedback cycle, which included holding the meeting, collecting feedback, incorporating feedback and preparing for the next meeting. Once the workgroup reached a consensus on its requirements, the workgroup's final requirements were submitted for approval through the governance structure illustrated in Figure 2.

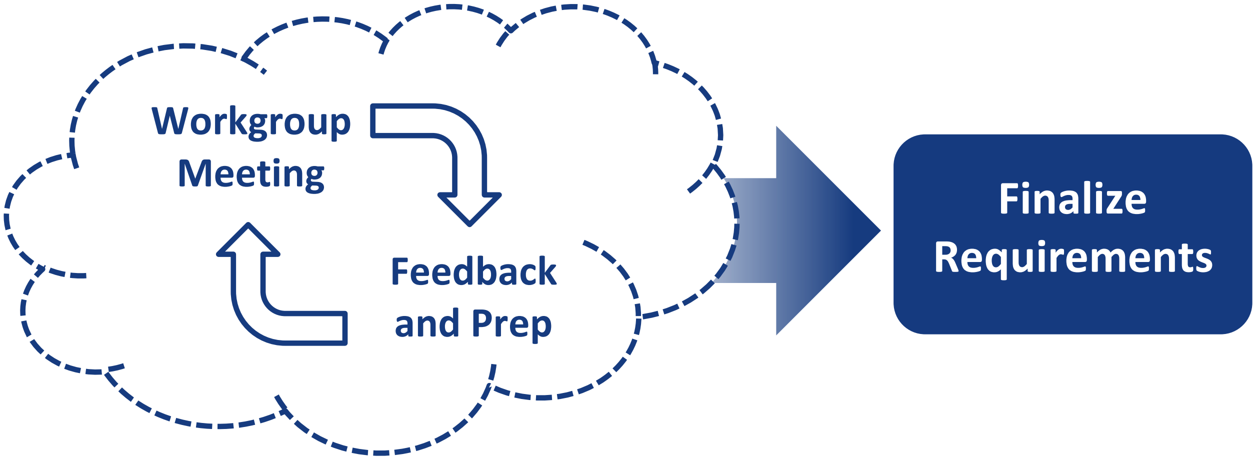


Figure 2: Workgroup Feedback Cycle

Participation

State requirements volunteers were initially recruited during outreach meetings held throughout early 2014, and through the state's existing contact lists for sheriffs, PSAPs, police chiefs and the State Emergency Communication Board's (SECB) announcements mailing list.

A total of 50 unique professionals participated in these workgroups including state staff, volunteers, and the MnFCP project staff including the workgroup facilitator. Many participants were involved in more than one workgroup providing for a total of **79 resources participating in the State's** requirements gathering process. For a full roster of workgroup Members, see Appendix 1.

[3] Available online at: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2609&file=BBWG_SoR_Launch_12112012.pdf

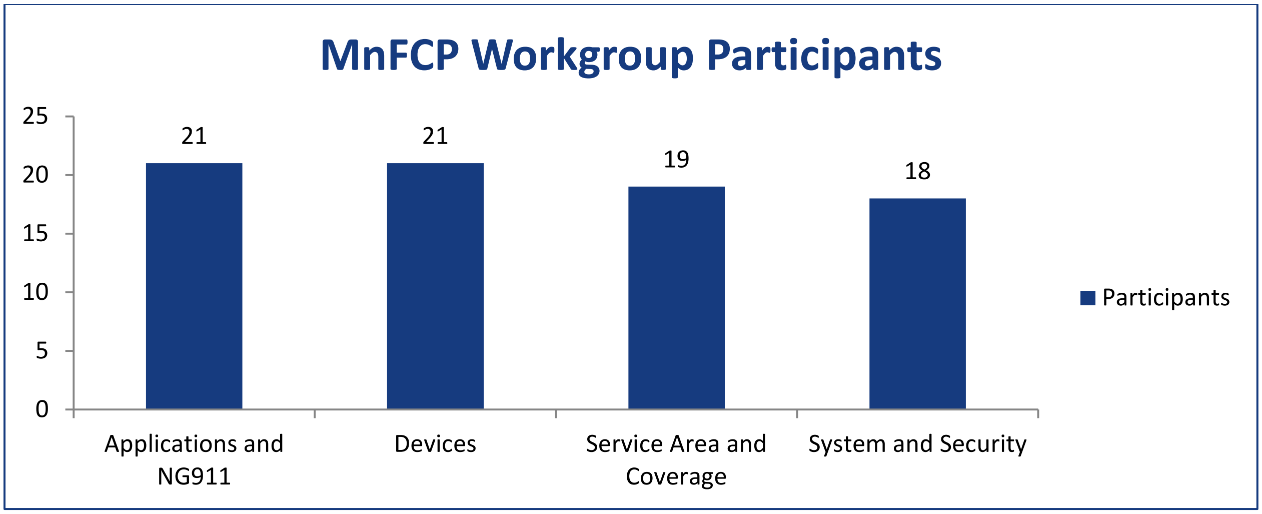


Figure 3: MnFCP Workgroup Participant Numbers

A majority of participating volunteers, a full 26 out of 50 people, represented county government. Following that, seven (7) participants represented State government, three (3) local government, three (3) nonprofits, three (3) MnFCP staff members, and no more than two in any other category.

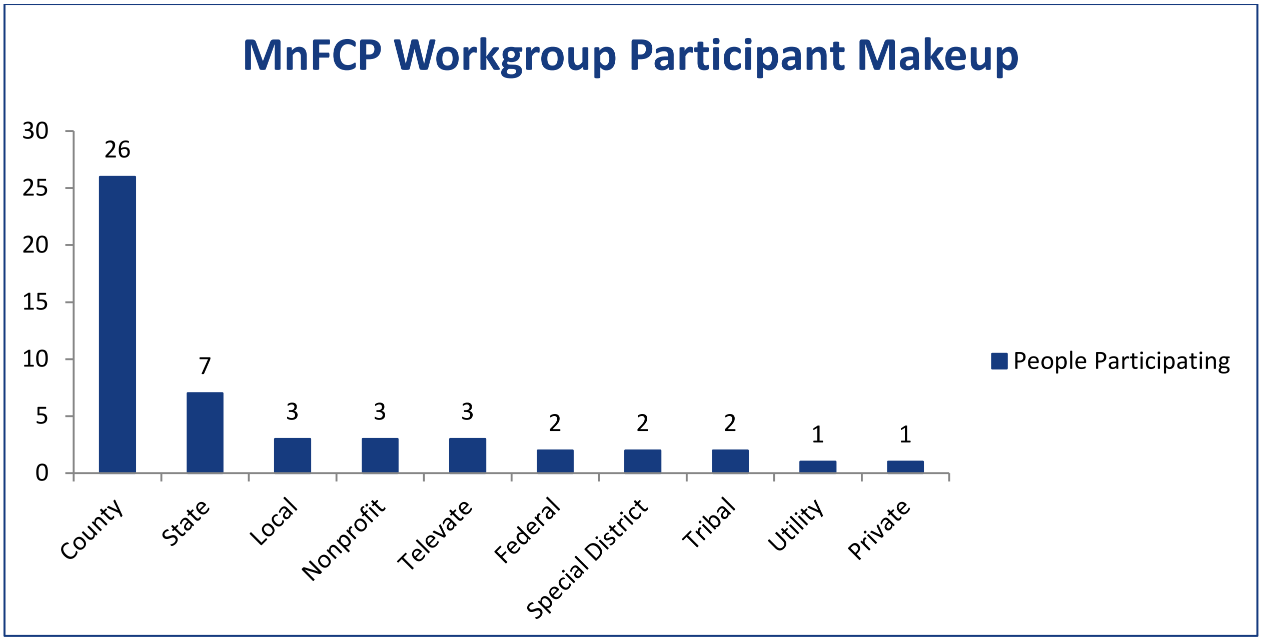


Figure 4: MnFCP Workgroup Participant Makeup

Applications and NG911 Requirements

Detailed Launch Requirements

For detailed launch requirements, please see the table Annex 1.

Workgroup Purpose

The purpose of the Applications and NG911 workgroup was to express Minnesota stakeholder user requirements for applications and NG911 on the NSPBN that would facilitate adoption of FirstNet services.

Key Findings

Applications inventory

The MnFCP project staff performed an applications inventory of membership agencies. In performing this inventory, the project team asked members of the community to describe the applications that they are currently utilizing with commercial or private mobile data networks. The objective of this exercise was to identify the types of information first responders are sending today to guide our future requirements development work.

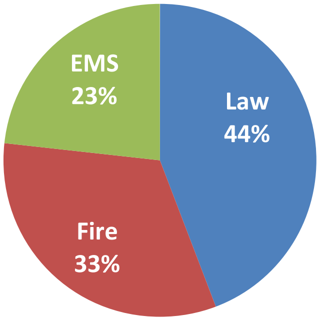


Figure 5: Application Distribution by Discipline

In total, 42 separate applications were surveyed. The team discovered that the predominant use case was a law enforcement user performing database queries, records management, and multimedia transfer related to the use of CAD system databases used for law enforcement. We were surprised to see that only one agency reported using video, and no agencies are using voice, in any capacity, over commercial mobile data networks.[4]

These findings represent the current state and represent application use only. While first responders do not report using field video right now, hundreds of surveys performed by the MnFCP project team in markets across the United States show that, over the long term and provided a highly reliable network, first responders demand the ability to utilize video in the field. For example, refer to the 2011 Minnesota Public Safety Data Network Requirements Study[5], which documents a high demand for incident video[6].

[4] "Voice" in this context does not include cellular telephony, and does include carrier services such as AT&T Enhanced Push-to-Talk (http://www.corp.att.com/enhanced-push-to-talk), or Verizon Push-to-Talk (http://business.verizonwireless.com/content/b2b/en/solutions/mobility/push-to-talk.html), as well as "over-the-top" services like Voxer (http://www.voxer.com/). Product mention does not imply endorsement.

[5] Available at https://dps.mn.gov/divisions/ecn/programs/armer/Documents/Minnesota_Needs_Assessment_Report_FINAL.pdf

[6] See Id. At pp. 32, 40-54

The applications findings illustrate that, at least at launch, throughput demands on the public safety network in Minnesota are likely to be relatively low, but that these throughput needs will escalate quickly as agencies take advantage of the multimedia capabilities of the network. Therefore, the NPSBN must be implemented to rapidly scale to meet the evolving capacity needs of public safety application adoption, which, driven by budgets and applications capabilities, is expected to occur within a short after launch timeframe. Our findings are illustrated in Figure 5 and Figure 6.

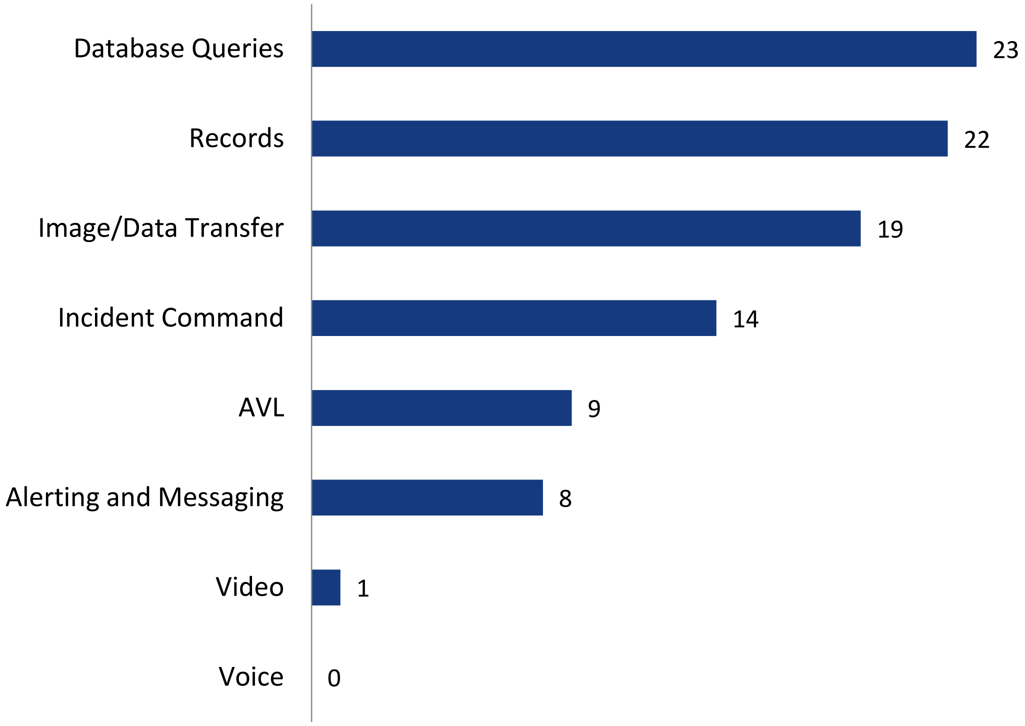


Figure 6: Data Type Utilization by Category

Deployment and Enablement

The workgroup reviewed NPSTC's deployment and enablement requirements for FirstNet. The group evaluated these requirements form four perspectives:

- Should FirstNet deploy the service at launch?
- Should FirstNet deploy the service at some point over the long-term?
- Should FirstNet enable (i.e., not block) the service at launch if an agency chooses to deploy it?
- Should FirstNet enable (i.e., not block) the service over the long term if an agency chooses to deploy it?

Minnesota's requirements in this area deviate from NPSTC's in that they add additional requirements. NPSTC provided only two requirements; (1) that FirstNet *deploy* the application, meaning FirstNet provides the service and/or the user application if appropriate, and (2) that FirstNet *enable* the application, meaning FirstNet:

- Does not block or interfere with the application or service
- Provides basic network services
- Provides IP connectivity
- Provides necessary priority and quality of service (QoS)[7]

Meanwhile, as detailed in Table 3, Minnesota includes five (5) categories within its requirements:

[7] See SOR at pg. 23

Table 3: Deployment and Enablement Terms and Definitions

Requirement	Description
Deployed by FirstNet at launch	FirstNet provides an interoperable service and end-user application to fulfill this requirement. Minnesota stakeholders expect that *every* NPSBN device in the state has this application installed and that any public safety user can reasonably expect that all public safety users have access to this application and service.
Enabled by FirstNet at launch	Per NPSTC; FirstNet does not block or interfere with the application or service, provides basic network services, provides IP connectivity *with neutral transport*, and provides necessary priority and QoS. Furthermore, FirstNet will provide the means to accommodate basic interoperability between different users and agencies utilizing this service.
Deployed by FirstNet long-term	Minnesota stakeholders do not expect this service to be available at launch, but Minnesota requires FirstNet's proposal to the State to include a timetable for deploying this service and the end-user application. We expect that *every* NPSBN device in the state has the ability to install relevant application(s) and access the service **by a specific date**.
Enabled by FirstNet long-term	Minnesota requires that FirstNet's proposal to the state includes a timetable for enabling this service (per the definition above) and provides a means to accommodate basic interoperability **by a specific date**.
Agency deploys end-user app	For services deployed or enable by FirstNet, whether the end-user agency installs and maintains the end-user application or whether it is provided by FirstNet. For those marked "No", Minnesota stakeholders expect that every device that functions on the NPBSN is provided to the user with this application installed and that the end-user or agency cannot uninstall it.

For the most part, the workgroup's requirements mirrored those of NPSTC. The workgroup's requirements are detailed in the table below:

Table 4: Minnesota Deployment and Enablement Requirements

Service	Definition	NPSTC: Deployed by FirstNet	NPSTC: Enabled by FirstNet	MN: Deployed by FirstNet at launch	MN: Enabled by FirstNet at launch	MN: Deployed by FirstNet long-term	MN: Enabled by FirstNet long-term	MN: Agency Deploys End-User App

Service	Definition	NPSTC: Deployed by FirstNet	NPSTC: Enabled by FirstNet	MN: Deployed by FirstNet at launch	MN: Enabled by FirstNet at launch	MN: Deployed by FirstNet long-term	MN: Enabled by FirstNet long-term	MN: Agency Deploys End-User App
Telephony (cell phone)	The ability to make telephone calls.	Yes	Yes	Yes	**Yes**	**Yes**	**Yes**	**No**
NG911 Emergency Services	The ability for the user application to interface with NG911 data sent to or generated by the PSAP.	Yes	Yes	No	**Yes;** pending NG911 service availability	**Yes;** pending NG911 service availability	**Yes**	**Yes**
CMAS/ IPAWS	The ability to receive CMAS alerts.	Yes	No	Yes	**No**	**Yes**	**No**	**No**
Messaging	The ability to send and receive text and multimedia messages (SMS/MMS)	Yes	Yes	Yes	**Yes**	Yes	**Yes**	**No**
Push-to-Talk Voice	Radio-style push-to-talk voice service; non mission-critical.	No	Yes	No	**Yes**	**Yes**	**Yes**	**Yes**
Mission-critical push-to-talk	Radio-style push-to-talk voice service; mission-critical.	n/a	n/a	**No**	**No**	**Yes**	**Yes**	**No**
Video Services	The ability to stream real-time video up and down from the scene; to easily and seamlessly share video as-needed.	No	Yes	**No**	**Yes**	**Yes**	**Yes**	**Yes**

Service	Definition	NPSTC: Deployed by FirstNet	NPSTC: Enabled by FirstNet	MN: Deployed by FirstNet at launch	MN: Enabled by FirstNet at launch	MN: Deployed by FirstNet long-term	MN: Enabled by FirstNet long-term	MN: Agency Deploys End-User App
Status "Web" Page	Web page where the user can assess the health of the network and any major announcements; resides on the network and does not require external internet access.	Yes	Yes	Yes	Yes	Yes	Yes	No
ARMER/P25 Interconnect; non-mission critical	ARMER seamless communications with the NPSBN	n/a	n/a	**No**	**Yes**	**Yes**	**Yes**	**Yes**
ARMER/P25 Interconnect; mission critical	ARMER seamless communications with the NPSBN	n/a	n/a	**No**	**No**	**Yes**	**Yes**	**No**

Striking all requirements related to Immediate Peril

NPSTC's SOR defines separate "emergency" and "immediate peril" functions.[8] The "emergency" function is to operate much like the emergency button on radios today, which would allow a user to initiate a call in an "emergency" state that provides heightened call priority and provides dispatchers and other personnel about a potentially life-threatening condition. The SOR's "immediate peril" classification, on the other hand, is intended to provide heightened priority to a call in the case that there is a threat to human life—presumably, a life other than the life of the user.

Workgroup members could not find a meaningful distinction between "emergency" and "immediate peril" calls. Members felt that a call either (1) **is directly related to** a life-threatening emergency, or (2) **is not directly related to** a life-threatening emergency. The workgroup rules to require one "emergency" call to handle **all** scenarios where there is the imminent threat to loss of human life.

[8] See SOR at pg. 41.

Further, the group felt that multiple different functions for priority traffic during a life-threatening event presented a training and User Experience (UX) challenge. Therefore, workgroup members elected to mark all requirements related to the “immediate peril” condition as “SHALL NOT”.

Devices Requirements

Detailed Launch Requirements

For detailed launch requirements, please see the table in Annex 1.

Workgroup Purpose

The Devices workgroup defines end-user device requirements, including mobile devices and routers. The group had a strong focus on mobile devices and not fixed devices, such as a computer terminal at a PSAP used for dispatch. Furthermore, the group focused on *cellular* devices; i.e., devices with an embedded cellular radio that operate on a cellular network. Devices, such as body-worn cameras paired via Bluetooth or LTE to a computer, smartphone or tablet were not considered cellular devices and are generally excluded from these requirements.

Key Findings

Among all device requirements surveyed from our workgroups, two stood out most prominently:

1. A strong desire for ruggedized handhelds, but little interest in currently-available rugged smartphone models.
2. A strong preference for existing form factors and commercial devices, and in particular Apple iOS and Stock Android devices.

Form Factor Requirements

We discovered that user agencies strongly desire ruggedized handhelds; these are devices capable of preventing intrusion of water and dust and withstanding shock and vibration.[9] However, during our workgroup sessions we determined that there was little interest in the existing rugged handhelds available on the market.

One workgroup member described having abandoned the Samsung Rugby Pro Smartphone (advertising certification as both IP and MIL-STD-certified for ruggedization)[10] from their agency's fleet in favor of Apple iPhones in water-proof, shock-resistant aftermarket cases.[11] The workgroup member justified this move in explaining that rugged smartphone models are always one or more generations behind in terms of technology, and that to keep current, the best approach was to utilize commercially available devices.

[9] Generally acceptable standards include United States Military Standards (MIL-STD) and International Electrotechnical Commission Ingress Protection (IP) certification processes. More information available respectively at http://www.atec.army.mil/publications/Mil-Std-810G/Mil-Std-810G.pdf and http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:1256.

[10] Product information available at: http://www.samsung.com/us/mobile/cell-phones/SGH-I547ZKAATT. Note that product information does not specify which ruggedization spec the device meets, e.g., IP-67; only that it meets "environmental protection an enclosure provides". Product mention does not imply endorsement.

[11] E.g., Otterbox; product information available at http://www.otterbox.com/. Product mention does not imply endorsement.

This interaction shows that while there is significant interest in ruggedized models, workgroup participants report that current technology is *more important* than rugged devices.

Table 5: Device Form Factor Requirements at launch

SHALL	SHOULD	SHALL NOT[12]	SHOULD NOT
Consumer Smartphone	Deployable Camera		Head-Worn Device[13]
Vehicular Router[14]	Remote Weather Sensor		Dual-mode[15] Handheld
Portable Router[16]	Remote-Controlled and Remote Multimedia Devices[17]		Fixed Camera[18]

[12] Workgroup members do not anticipate at this time, any devices currently available on the market or device features in known 3GPP standards that would, in **all cases**, be harmful to the network. However, workgroup members strongly support the state's governance structure exercising the right of refusal for any future device categories from operating on the NPSBN in the state.

[13] A head-worn smart device such as the recently-discontinued Google Glass prototype. While workgroup members did not challenge the utility of this device category, there was little to no interest among workgroup members in this category of device for launch window of the service.

[14] An LTE router that supports multiple devices, from 2-3 to over 100 in some applications. Typically installed in a vehicle, e.g., a patrol car. Occasionally installed on a fixed or temporary fixed basis such as at an emergency operations center.

[15] A mobile device with an embedded P25 and analog radio. Note that there was very little interest in this category among workgroup participants.

[16] E.G., "puck" form factor mobile hotspot.

[17] Workgroup members anticipate a strong desire for body-worn cameras and microphones, as well as other remotely controlled devices like drones, that would use direct-mode LTE for the link between the remote device and a cellular-connected device like a smartphone or computer, instead of connections over unlicensed spectrum like WiFi and Bluetooth.

[18] Workgroup members objected to fixed multimedia cameras, such as IP CCTV systems, being deployed on the network because they could significantly contribute to network congestion. Workgroup members felt that the NPSBN should not be considered a viable means for backhauling fixed multimedia traffic as it would contribute to network congestion, and that alternative methods for backhaul, including Ethernet and microwave, are preferred.

SHALL	SHOULD	SHALL NOT[12]	SHOULD NOT
Consumer Tablet			Wearable Multimedia Device[19]
Laptop			
Sensor/M2M			

The delay in the availability of current generation devices introduces a dilemma to device manufacturers and network operators; users have an expressed need for current commercial technologies, but specialized mobile devices designed specifically for rugged environments have historically lagged behind the current pace of technology. In order to ensure maximum adoption, the network operator should identify some means to stay lock-step with commercially-available mobile platforms while meeting public safety needs for ruggedization.

This point is further illustrated in Table 5: Device Form Factor Requirements above; when evaluating existing and potential form factors, the only *required* ("shall" in the table below) form factors were existing, commercially-available platforms such as consumer smartphones, while potential form factors not currently on the market were only classified as *desired* ("should" below) by the workgroup. The takeaway is very clear; the network operator will need to support existing commercial platforms in order to be a success at launch.

Mobile OS

Though the workgroup requirements focused on *what*—what the need is, versus *how*—what would satisfy that need, the workgroup felt that it was appropriate to specify that **Apple iOS and Stock Android devices are required on the network**; meaning, they do not support a service that does not support these two very popular smartphone platforms.

Workgroup members reported that iOS was the dominant mobile platform in their fleets, and Android was a distant second. Workgroup members agreed that overall adoption would be very low if Apple and Stock Android[20] devices were not supported on the NPSBN. Members reported little utilization of other mobile OSes in their fleets such as Blackberry or Palm OS.[21] In the interest of promoting a high adoption

[19] Workgroup members do not anticipate a desire for body-worn cameras and microphones that have their own, dedicated cellular connection. Workgroup members believe desire for these devices will be as peripherals or accessories connected to a smartphone, tablet, computer or other device that provides a connection to the NPSBN.

[20] "Stock Android" in this case means mobile devices running the Android operating system with minimal to no modification to the base Android operating system.

[21] Mobile OS use was not inventoried as part of the workgroup projects, but this topic was addressed as a separate task under the MnFCP. See https://dps.mn.gov/divisions/ecn/Pages/broadband.aspx.

rate, the workgroup felt confident to (1) require adherence to commercially-available mobile operating systems, (2) forbid an NPSBN-specific mobile OS, and (3) require that Apple iOS devices are available on the service.

There is no technical need driving this requirement; meaning, there is no bona fide technical reason that iOS and Android OS are the only mobile operating systems that could meet public safety's needs in Minnesota. The workgroup voting to require devices that support iOS and Android is an acknowledgement of the business reality of today's mobile devices—if the network does not support the most popular devices in the commercial market, adoption rates in the state will be precipitously low and the service will likely not be sustainable in the state.

Note that as of this writing, current iOS devices (Apple iPhone6 and Apple iPad Air 2) do not offer models supporting LTE Band 14.[22]

Impediments to Adoption

The devices workgroup evaluated what its members felt would be the most significant impediments to adoption based on end-user experience. Workgroup members evaluated impediments to adoption from the perspective of what would make it difficult for them, as technical experts, to advise that their agency take up FirstNet services. While all of these impediments correspond or mirror the detailed requirements included Annex 1, the workgroup prioritized high-profile barriers and provided suggested solutions. These impediments are detailed in Table 6: Impediments to Adoption below.

Table 6: Impediments to Adoption

Impediment	Description	Impacts to Adoption	Suggested Solutions
Network Cost	Cost-competitiveness with alternatives including commercial carriers and enterprise-owned networks.	Lowered adoption	Compete with commercial device and service costs and justify any increased cost with better performance.
Enterprise Management	Control over device and application management, such as on agency WANs and/or carrier enterprise agreements today.	Low/No adoption	Devices certified to operate on FN's network must enable enterprise management including application installs, device image, remote stun/kill, A/D integration, etc.
Training	Effort required to train responders in the use of new devices and applications.	Delayed adoption	Offer market-leading commercially-available devices; specifically Apple iOS

[22] See https://www.apple.com/iphone-6/specs/ and https://www.apple.com/ipad-air-2/specs/. Per https://www.apple.com/iphone/LTE/ and https://www.apple.com/ipad/LTE/, Apple does not offer LTE Band 14 in any of their devices today.

			and Android devices
Legacy Platforms	Support for Android and iOS devices in-use today. Agencies have invested in applications, training, accessories, etc. in these platforms.	Lowered adoption Delayed adoption	Offer market-leading commercially-available devices; specifically Apple iOS and Android devices
Platform Consistency	Platform consistency where a lack thereof may introduce issues with SOPs, application availability or interoperability. For emample, if there are multiple operating systems, the same suite of applications may not be available for all of them.	Lowered adoption	Offer market-leading commercially-available devices; specifically Apple iOS and Android devices
Form factor/ UX	Quality of industrial and software design as compared to commercial alternatives.	Low adoption	Offer market-leading commercially-available devices; specifically Apple iOS and Android devices
Commercial Roaming	Support for all major cellular carriers as roaming partners.	Lowered adoption	Support all major cellular carriers through device options. For example, AT&T may have better coverage in County A, Verizon may have better coverage in County B, T-Mobile in County C and Sprint in County D. In this example if only one of these carriers were supported as a roaming partner statewide, only one of these four counties would likely be satisfied with NPSBN service. The other three may not migrate or may migrate later.[23]

[23] This factor is not evaluated objectively in this report, but is evaluated on a county-by-county basis as a separate arm of the Minnesota-FirstNet Consultation Project. See https://dps.mn.gov/divisions/ecn/Pages/broadband.aspx.

Service Area and Coverage Requirements

Detailed Launch Requirements:

For detailed launch requirements, please see the table in Annex 1.

Workgroup Purpose

The coverage workgroup defined the standards through which coverage offered by the NPSBN is evaluated. Additionally, the workgroup provided guidelines for individual stakeholder coverage reviews.

Key Findings

Service Area Classification

The Coverage workgroup defined three classifications of service areas for the purposes of expressing requirements. These areas are (1) Critical Service Area, (2) Required Service Area and (3) Extended Service area. A visual example is shown in *Figure 7: Example Service Area Requirements, Stearns County MN* below.

1. **Critical Service Area**
   This area is defined as the area of highest activity for the agency, any areas with critical infrastructure, and any major freeways or thoroughfares. In these areas, agencies expect highly reliable in-building service on dedicated BC-14 spectrum. Areas of high activity for each agency are justified empirically using historical CAD/RMS data from each PSAP.
2. **Required Service Area**
   This area is defined as the area currently covered by cellular carriers[24] to agencies today, minus any critical service areas. In the case of population centers and major highways, it is likely that much of this area overlaps with the "Critical" service area. There is no expectation that at launch there will be highly reliable service on dedicated BC-14 spectrum within this geography, and that at launch, coverage will be primarily provided through a roaming partner. It is acceptable, for example, that at launch these areas are covered through a commercial partner. The purpose for this category is that, in order to compel users to switch to the public safety network, it must *at least* exceed the service provided today through a commercial option.
3. **Extended Service Area**

   This area is categorized by current coverage provided by the agency's private wireless services, such as their land-mobile radio and paging systems, as well as any remaining gaps commercial carriers do not cover. In practice, the "extended" area will cover all of the agency's geography. There is expectation that some of these areas would be covered at launch, or the program to

[24] Note—for each coverage review, the MnFCP project team compared to the cellular carrier that agency uses. For example, if the interviewee agency was a Verizon customer, the survey would compare to Verizon coverage. If the agency utilized three different commercial carriers, all three of the carriers that the agency utilized were compared.

begin planning for coverage in these areas would begin at launch[25], and providing at least mobile coverage in these areas provides added value. For example, if the network provided coverage to these areas the agency could consider replacing a private paging system with a mobile service.

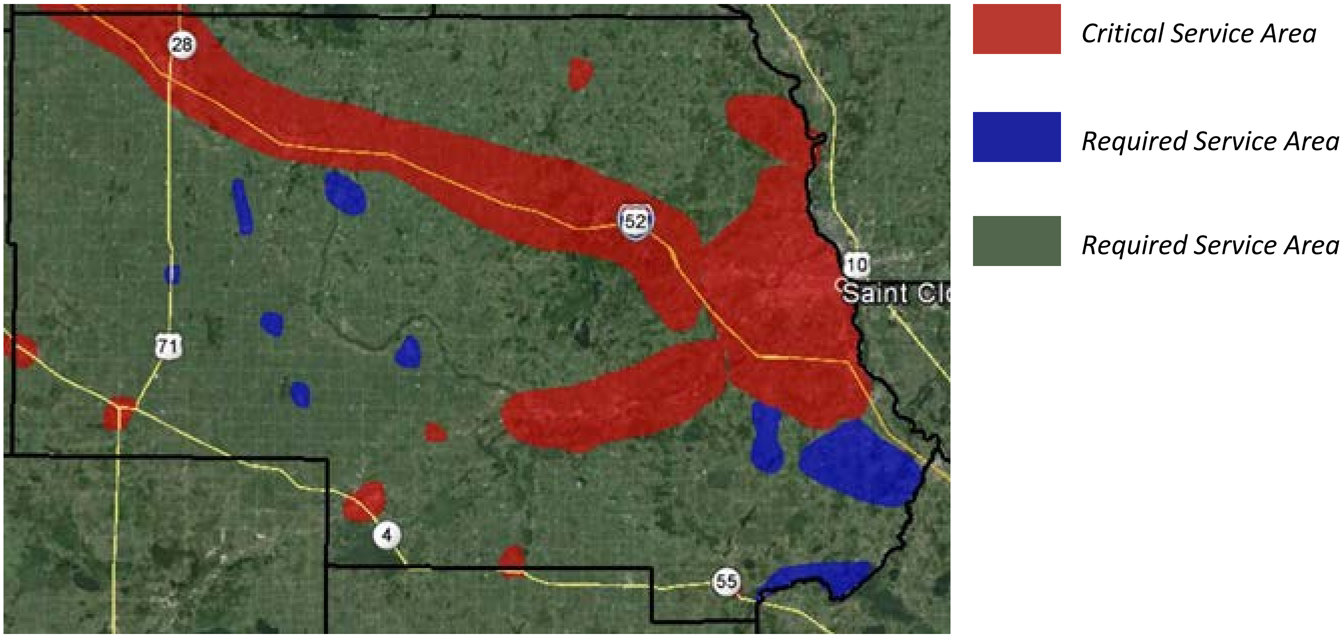


Figure 7: Example Service Area Requirements, Stearns County MN

Commercial Failover Required

Notably, the workgroup expressed that commercial failover is a required feature. The public safety network must be able to failover to a commercial technology to provide an added layer of redundancy. For example, the workgroup's Minneapolis delegate cited experience using a citywide Wi-Fi network for first responders throughout the city coupled with commercial service from all four major carriers, depending on which provided better service in that particular unit's area of operation. The delegate reported that while coverage and reliability did not fully meet their agency's needs on either network alone, they were able to meet Minneapolis' needs by using both private and commercial data services in tandem. This experience led the workgroup to declare commercial failover as a required feature statewide for the network.

Data Throughput and In-Building Coverage

Throughput: FirstNet must provide:

- A minimum of 4 Mbps (DL) and 1 Mbps (UL) for a single user over 95% of each Critical Service Area for each county

[25] As of the release of this report, the workgroup is defining the state's phased coverage requirements, and there is expectation that some percentage of underserved and unserved commercial coverage areas would be covered in each of the rolling coverage phases.

- Single user throughput equivalent or greater than typical commercial carrier service in all other areas (RSA and ESA) but not less than 756 kbps DL and 268 kbps UL in any area where coverage is required.

In-Building Coverage

- FirstNet should provide in-building coverage that delivers a minimum of 256 kbps uplink to a body worn portable device for 95 % of the interior of each building (includes above and below ground areas).

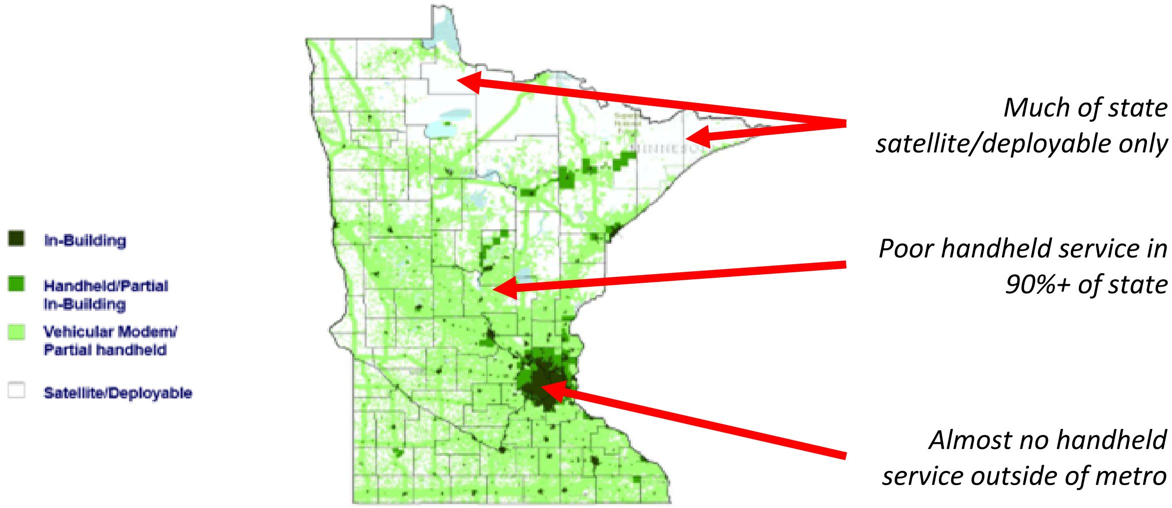
Criteria	Weight	Minimum Acceptable Req.	Objective/Goal
Coverage	**20%**		
•Quality (indoor / outdoor, Mbps, seamless)	5%	Vendor shall provide sustainable indoor coverage and throughput equivalent to commercial grade service. Vendor shall provide for roaming on all indoor solutions via roaming as a minimum, but must provide Band 14 indoor DAS solutions for all major venues including stadiums, arenas and convention centers. Vendor shall provide service that transitions between Band 14, and roaming coverage must be seamless for all devices including hand held form factors.	Vendor should provide throughput that leverages capacity from other spectrum bands (non-Band 14) to address the net capacity needs of public safety in a major emergency. The vendor should provide indoor service levels and throughput per as described in the State of Minnesota Build-Out Strategy and Priorities document.

Workgroup Opinion on the OEC Coverage Model

The workgroup was not comfortable with the Department of Homeland Security (DHS), Office of Emergency Communication's (OEC) coverage model prepared for the State under the OEC Technical Assistant Program[26]. The workgroup expressed three primary reasons for their dissatisfaction with the model; (1) poor rural coverage; (2) poor in-building coverage, and (3) the belief that satellite and deployable systems are not acceptable for routine operations.

[26] FirstNet has recently indicated that the OEC coverage map now serves as a framework for the state to reference when developing its phased coverage recommendations to FirstNet.

In general, the workgroup's thoughts were unified by the experience that they receive better service through a commercial carrier today than was offered by OEC's model. Accordingly, they would have little incentive to migrate to the public safety network if it offered the coverage provided by OEC's model, or by baseline coverage model substantially similar to OEC's model.


In-Building
Handheld/Partial In-Building
Vehicular Modem/ Partial handheld
Satellite/Deployable

Much of state satellite/deployable only

Poor handheld service in 90%+ of state

Almost no handheld service outside of metro

Figure 8: Workgroup Criticism of OEC Coverage Model

The workgroup's three primary areas of concern are detailed below:

1. **Poor rural coverage**.
   Throughout approximately 90% of the state, OEC's model illustrated "vehicular modem/partial handheld" coverage with approximately half of the rural landmass showing "satellite/deployable". The workgroup felt this level of coverage was unacceptable to meet their needs and in most cases worse than service available to them from a commercial carrier.

2. **Poor in-building coverage.**
   OEC's benchmark for "in-building coverage" is a coverage that "provided to a handheld device through minimum one wall". Metropolitan-area members of the workgroup felt that this was inadequate to meet their needs where cellular providers and building owners provide much greater coverage through distributed antenna systems, BDAs and picocells.

3. **Satellite/deployables are not an acceptable alternative for routine operations.**
   Rural-area members of the workgroup reported that satellite and deployable systems are not acceptable for routine operations. They cited experience using satellite systems and in particular that they were high-latency and weather dependent and can take hours to set up. Additionally, they provided experience being unable to obtain a clear view of the southern sky in heavily-forested areas throughout northern Minnesota. While deployables will be required, deployment is not trivial and the workgroup did not accept them as a preferred option.

System and Security Requirements

Detailed Launch Requirements

For detailed launch requirements, please see the table Annex 1.

Workgroup Purpose

The Minnesota and FirstNet Consultation Project (MnFCP) workgroups defined Minnesota's requirements for System and Security for the Minnesota and FirstNet consultation process. The group's focus was to review NPSTC requirements on information security and any special architectural needs to support interoperability.

Key Findings

The System and Security workgroup reviewed a greater extent of the NPSTC's launch requirements than any other Minnesota workgroup. The workgroup identified a total of 45 new requirements or modifications to NPSTC's base requirements. The issues identified centered on security practices, a consistent theme that FirstNet should leverage existing commercial platforms, and that FirstNet must make firm commitments to meet agency requirements through an SLA.

The NPSBN is an Untrusted Network

Workgroup member requirements carry a consistent message that FirstNet should not be responsible for ensuring the security of individual agency data that crosses the network. In the view of workgroup members, **the NPSBN is an Untrusted Network**. The user agencies plan to take the same security precautions — e.g., VPN and end-to-end encryption — that they conduct over commercial networks today. Therefore, that FirstNet delivers a highly secure network is, in and of itself, likely to provide a compelling reason to adopt the service for Minnesota stakeholders. End-user agencies will assume that the FirstNet broadband network was not more secure than any other publicly-accessible network they share with consumers today.

Table 7: Encryption Requirements

#	Description	SOR	MN	Comments
MN-20	PSEs SHALL be able to manage encryption of traffic on the client side without modification or interruption to public safety traffic.	N/A	SHALL	

SOR-108.4	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.	SHALL	SHALL WITH COMMENTS	*The responsibility to ensure all sensitive traffic is encrypted end-to-end rests on the operating agency.*
SOR-108.5	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.	SHALL	SHALL WITH COMMENTS	*Workgroup assumes that the non-FirstNet UE in this requirement is accessing an NPSBN service or application over a commercial network. Otherwise, this requirement would not apply.*

FirstNet Must Match the Level of Coverage and Throughput Provided by Commercial Carriers

Central to requirements for the NPSBN are the level of coverage and throughput provided by the service. Rather than provide a specific metric, however (e.g., a percentage of geography or a specific bit rate throughput), the workgroup elected to base its requirements for coverage and throughput upon the standards established by incumbent commercial carrier services. In general, the workgroup's requirements for coverage and throughput are that they be equal to or better than what users presently have available through commercial carriers. Workgroup members felt that, if the service is not better than commercial wireless services that users in Minnesota have today, there will be little incentive for public safety agencies to migrate to the service.

Table 8: Commercial Carrier Requirements

#	Description	SOR	MN	Comments
MN-02	The network operator SHALL provide throughput speeds per-user that meet or exceed speeds available through commercial carrier services.	N/A	SHALL WITH COMMENTS	*This is a subjective measurement, but the intent is that the user experience on the NPSBN is for throughputs at least equivalent to carrier services.*
MN-10	The network operator SHALL provide coverage generally better than coverage available through commercial carrier services.	N/A	SHALL	

FirstNet Must Secure the Consent and Approval of Minnesota's Governance Structure

The System and Security Workgroup reviewed NPSTC's requirements focused on governance. The workgroup took the position that the state's governance structure must be empowered to make policy decisions related to use of the NPSBN, including **who should be considered an eligible user**.

This position is supported by Minnesota Statute, which specifies that the SECB is responsible for developing and maintaining "a plan for implementation of the NPSBN and to define technical and operational standards for the network."[27]

Significantly, the workgroup took the position that Minnesota's governance structure SHALL determine the requirements to qualify as a user.[28] As a "SHALL" requirement, this carries great significance: it means that Minnesota will not accept a State Plan that does not allow the governance structure to determine what constitutes an eligible user of the network.

SECB and RECB/RESBs in Minnesota have substantial capability to support buy-in throughout the state at a highly granular level. The governance structure also provides an avenue to enforce compliance with standards and advocate for best practices, as well as to adopt standards and best practices with a high degree of stakeholder ownership.

A coordinated governance structure across the state can manage conflicts regarding use of the network, abuse of network privileges and to coordinate special events across separate levels of government and with non-governmental user entities.

Additionally, because RECB/RESBs are legal entities with the ability to enter into contracts and own property, they represent valid potential business partners or VMNO entities.

Table 9: Governance Requirements

#	Description	SOR	MN	Comments
MN-38	Minnesota's governance structure SHALL determine the requirements to qualify as a user.	N/A	SHALL	*FirstNet is required to coordinate with the SECB under Minnesota statute. See MN Stat. 403.382 Subd. 8 Sec. 1.*
SOR-1.1	FirstNet SHALL define the requirements for agencies and/or authorities to qualify as NPSBN users.	SHALL	SHALL NOT	*See MN-38.*

[27] *See* MN Stat. 403.382 Subd. 8 Sec. 1.

[28] *See* MN-38.

SOR-2.1	FirstNet SHOULD collaboratively leverage existing statewide communication governance models to incorporate the input of the entire local, tribal, state, and federal community.	SHOULD	SHALL	*See MN-38.*
SOR-2.2	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.	SHOULD	SHALL WITH COMMENTS	*See MN-38.*

Location Services are Required

The NPSTC SOR identified enhanced autonomous location services as optional.[29] The workgroup felt that location services are absolutely essential to the public safety mission and elected to change the associated requirement to “SHALL”.

Table 10: Location Requirements

#	Description	SOR	MN	Comments
SOR-67.3	NPSBN UE SHOULD support enhanced autonomous location services (e.g., latitude, longitude).	SHOULD	SHALL	*Location services are* ***required****, not requested.*

Access to Commercial Networks is Required

The SOR designates access to commercial networks as a desired feature, but not a required one for all classes of device.[30] The workgroup strongly disagreed and reclassified SOR requirements addressing commercial network access as required (“SHALL”) and not desired (“SHOULD”).

[29] *See* SOR-67.3: NPSBN UE SHOULD support enhanced autonomous location services (e.g., latitude, longitude).

[30] *See* SOR-66.1, 66.2, 66.3, 66.4

Table 11: Commercial Network Access Requirements

#	Description	SOR	MN	Comments
SOR-66.1	NPSBN-Us SHOULD have consumer-equivalent smartphones capable of operating on both commercial networks and the NPSBN.	SHOULD	SHALL	*Workgroup members feel there will very little interest in a service that does not provide access to commercial networks.*
SOR-66.2	NPSBN-Us SHOULD have consumer-equivalent tablet PCs capable of operating on both commercial networks and the NPSBN.	SHOULD	SHALL	*Workgroup members feel there will very little interest in a service that does not provide access to commercial networks.*
SOR-66.3	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.	SHOULD	SHALL	*Workgroup members feel there will very little interest in a service that does not provide access to commercial networks.*
SOR-66.4	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).	SHOULD	SHALL	*Workgroup members feel there will very little interest in a service that does not provide access to commercial networks.*

SLA Requirements

While the Minnesota Launch Requirements could be considered as a *whole* to generally describe the state's SLA requirements before FirstNet, the workgroup did identify a number of specific requirements that its members felt were particularly important to the terms of its required SLA. Those requirements are detailed in the table below.

Significantly, the workgroup established the requirement that, in general, "The service provider SHALL provide an SLA that meets or exceeds all requirements in Minnesota's Statement of Requirements document."[31] This requirement is intended to communicate that, in general, the Minnesota Statement of Requirements document specifies the minimum acceptable terms from an SLA provided by FirstNet.

[31] *See MN-00*

Table 12: SLA Requirements

#	Description	SOR	MN	Comments
SOR-61.7	To ensure a reasonable end-to-end quality of service, performance level benchmarks SHOULD be included in roaming agreements between FirstNet and commercial carriers.	SHOULD	SHALL	*Workgroup finds it highly unlikely that FirstNet would enter into a roaming agreement without an agreed-upon performance level benchmark, even if that benchmark is "best effort".* *Workgroup members also feel their agencies would need to know the level of service when roaming off of FirstNet, as opposed being a regular customer of that roaming partner, much as they would today when assessing a VNMO entity.*
MN-00	The service provider SHALL provide an SLA that meets or exceeds all requirements in Minnesota's Statement of Requirements document.	N/A	SHALL	
MN-04	The service provider SHALL include in its SLA response times for outages and network trouble.	N/A	SHALL	
MN-05	The service provider SHALL include in its SLA response times for deployable fill-in sites such as Cell-on-Wheels (COW) and Cell-on-Light-Truck (COLT).	N/A	SHALL	
SOR-17.1	FirstNet SHOULD develop a policy defining the ability and process for local, tribal, state, and federal entities to monitor the network.	SHOULD	SHOULD WITH COMMENTS	*SOR requirement does not define what "monitor" means and what is being monitored.*

SOR-17.2	FirstNet SHALL establish policies to provide user entities prompt trouble reports, information helpful to facilitate operations using contingency communications, and restoration reports.	SHALL	SHALL WITH COMMENTS	*State Plan SHALL detail SLA terms that will include trouble response windows and reporting requirements.*
SOR-17.3	FirstNet SHALL establish a policy to provide user entities insight into overall system performance metrics, including availability and coverage.	SHALL	SHALL WITH COMMENTS	*State Plan will detail SLA terms which will include reporting required from the network operator.*

FirstNet should consider Deploying Band Class 14 Network as Secondary to Commercial Networks in Minneapolis

The City of Minneapolis' delegate reported no need for an increased level of service compared to commercial carriers in Minneapolis during routine operations, reporting no material issues with coverage, network congestion or downtime. The Minneapolis delegate reported that the most significant value to the city would be the availability of BC14 dedicated spectrum *during a major incident*, citing, for example, the 2008 I-35W bridge collapse.

During those special circumstances, the delegate sees tremendous value in separating public safety spectrum from a greater public pool to support lifesaving operations. During routine activities, however, the city's delegate did not see great value in an alternative service unless that service met or exceeded the commercial services the city is using today. This report is consistent with the workgroup's broader message: that FirstNet must use the commercial carrier service that public safety agencies are very happy with using already as their baseline requirement.

FirstNet Should Offer its Services through pre-existing Contracts

Workgroup members reported purchasing cellular service predominantly through the Cooperative Purchasing Venture (CPV) program,[32] which allows eligible entities including governmental entities, charitable organizations, community clinics and other entities to purchase goods and services from contracts established by the State through MMD (Materials Management Division). In Minnesota wireless services is available by a variety of carriers under state contract,[33] and agencies reported a strong desire to order FirstNet's services through a pre-negotiated state contract in the same manner. A small minority of workgroups also reported purchasing wireless service through GSA.

Accordingly, the workgroup saw fit to recommend that FirstNet establish a pre-negotiated purchasing contract through MMD to enable it to easily provide its services to public safety agencies. To a lesser extent, the workgroup also recommends that FirstNet establishes a GSA master rate schedule.

[32] *See* Minn. Stat. § 16C.03, subd.10.

[33] *See* Minn. Contract Release T-535(5), "Wireless Services"

Table 13: Purchasing Contract Requirements

#	Description	SOR	MN	Comments
MN-36	FirstNet SHOULD establish a master contract with the state of Minnesota to make ordering devices and service easier for end-user agencies.	N/A	SHOULD	*See SOR 19.3.*
MN-37	FirstNet SHOULD establish a master contract with US General Services Administration to make ordering devices and service easier for end-user agencies.	N/A	SHOULD	*See SOR 19.3.*
SOR-19.3	FirstNet SHALL provide support for procurement of goods and services.	SHALL	SHALL WITH COMMENTS	*Most agencies in Minnesota currently order cellular services and devices off of state and GSA schedules.*

Lessons Learned

Seek Input from many Levels of Government

The workgroups included participants from federal, county, local, state and tribal government, nonprofits, volunteers and the private sector. However, county governments were significantly represented in the workgroups, accounting for more than half of the participants in the workgroups and nearly four (4) times as many participants than any other member category. Local government was significantly under-represented in our sample, with only three (3) members contributing on behalf of a city, village or township, and not every city of first class represented.[34]

However, officials participating on behalf of county government do substantially represent the political subdivisions within that county. Further, government entities participating contained a highly diverse sample of metropolitan areas,[35] rural areas,[36] and areas with a mix of both.[37] Therefore, although we did not have substantial participation from cities, villages or townships we have a high degree of confidence that our requirements development has a reasonable balance rural and metropolitan input.

Seek a variety of Inputs from Outside of State Government

The state government ultimately has right of refusal regarding FirstNet's deployment in the state.[38] However, the state government represents a minority of Minnesota's user base for NPSBN services—most public safety officials represent local and county government. We sought requirements from these stakeholder groups because they represent most of the future users of NPSBN services. This workgroup composition provided a high degree of confidence that our requirements represents a large proportion of the state's future user base.

Consolidate Workgroup Scope

We found that the same individuals often participated in several workgroups, and that our most active members were part of all workgroups. While the intention was to initially commission five workgroups, the number was reduced to four by combining the System and Security workgroups. Even then, we found a high degree of redundancy between different workgroups. We expect that a similar outcome would have resulted with a smaller number of workgroups—potentially even with a single, broadly-scoped workgroup.

[34] Two cities of first class, St. Paul and Rochester, did not have delegates on the workgroups.

[35] E.g., City of Minneapolis, Hennepin County and City of Duluth

[36] E.g., Lake County, Polk County and White Earth Nation

[37] E.g. St. Louis County, Washington County, and Stearns County

[38] The governor of each state reviews FirstNet's plan and determines whether or not to approve that plan and has the opportunity to develop an alternative plan to build the radio access network in their respective state. See http://firstnet.gov/consultation.

Annex 1: Statement of Launch Requirements

The table below is available as an .xlsx file, MN_NPSBN_Launch_Requirements_2015-06-22.xlsx.[39]

Important Note about Document Version 1

This version of the document does not include most of the requirements vetted by the System and Security Workgroup.

How to Read the Requirements

This table includes the following fields:

#

The requirement number. "MN-x" numbers are unique, Minnesota-specific requirements developed by the State's workgroups. "SOR-x" numbers are requirements from the NPSTC SOR reviewed by the workgroup.

Description

The full text of the requirement. For "SOR" numbers, this text is copied from the SOR. If the workgroup has a new requirement or an amendment to an SOR requirement, the change(s) will be included in the description of an "MN" requirement. "MN" requirements are either new requirements or those where the group felt the SOR did not adequately address the State's need.

SOR

The directive ("SHALL", "SHOULD", "SHOULD NOT" and/or "SHALL NOT") from the text of the NPSTC SOR. In cases where the SOR requirement included more than directive, we used the most important one.

MN

Minnesota's requirement as determined by the workgroup.

Comments

Any special qualifications from the workgroup, such as (and typically) the reasoning behind deviating from the SOR.

Comp.

Whether "SOR" and "MN" fields match. Provided for quick reference purposes.

[39] Available at https://dps.mn.gov/divisions/ecn/Pages/broadband.aspx.

#	Description	SOR	MN	Comments	Comparison
MN-00	The service provider SHALL provide an SLA that meets or exceeds all requirements in Minnesota's Statement of Requirements document.	N/A	SHALL		N/A
MN-01	The NPSBN SHALL prohibit push-to-talk voice services that are not interoperable with other push-to-talk voice services on the network and that are not developed in accordance with 3GPP Standards.	N/A	SHALL		N/A
MN-02	The network operator SHALL provide throughput speeds per-user that meet or exceed speeds available through commercial carrier services.	N/A	SHALL WITH COMMENTS	*This is a subjective measurement, but the intent is that the user experience on the NPSBN is for throughputs at least equivalent to carrier services.*	N/A
MN-03	The NPSBN operator SHALL be held to the same regulatory requirements as a commercial cellular carrier for the purposes of service quality and 911 service.	N/A	SHALL		N/A
MN-04	The service provider SHALL include in its SLA response times for outages and network trouble.	N/A	SHALL		N/A
MN-05	The service provider SHALL include in its SLA response times for deployable fill-in sites such as Cell-on-Wheels (COW) and Cell-on-Light-Truck (COLT).	N/A	SHALL		N/A
MN-06	The service SHALL support mobile hotspots.	N/A	SHALL		N/A
MN-07	The service SHALL support mobile tethering.	N/A	SHALL		N/A
MN-08	Roaming charges SHALL be included in the price provided to public safety users without a separate usage surcharge incurred when users are roaming off of the service.	N/A	SHALL		N/A
MN-09	The NPSBN SHALL positively and uniquely identify the user prior to establishing any call including an emergency call.	N/A	SHALL WITH COMMENTS	*Note: This does not apply to a 911 call.*	N/A
MN-10	The network operator SHALL provide coverage generally better than coverage available through commercial carrier services.	N/A	SHALL		N/A
MN-11	The network operator SHALL provide coverage benchmarks, with specific deployment timetables, for "rural" areas of the state. The term "rural" is to be interpreted by the state's governance structure, and the governance structure SHALL have significant control over how rural benchmarks are met. "Governance Structure" is as defined in MN Stat. 403.	N/A	SHALL		N/A
MN-12	The network operator SHALL provide coverage maps depicting which areas are covered exclusively by Band 14.	N/A	SHALL		N/A
MN-13	The network operator SHALL provide coverage maps depicting which areas are covered both by Band 14 and by its roaming partner(s) on other spectrum bands.	N/A	SHALL		N/A
MN-14	The network operator SHALL provide coverage maps depicting which areas are covered exclusively by roaming partner(s) and not covered by Band 14.	N/A	SHALL		N/A
MN-15	The service provider SHALL depict, in its coverage maps, which areas include indoor coverage, outdoor handheld coverage and outdoor mobile coverage.	N/A	SHALL		N/A
MN-16	The service provider SHALL provide unambiguous engineering values used to generate its coverage maps.	N/A	SHALL		N/A
MN-17	The service provider SHALL provide coverage maps at launch which show the network operator's target Final-Operating Capability (FOC). The intent is for public safety agencies to include current coverage in their long-term communications	N/A	SHALL WITH COMMENTS	*Subject to change; but MN requires that agencies have timetables and targets to plan their own investments and transitions around.*	N/A

	planning efforts, including when to adopt the service. Note: Maps SHALL include a reasonable degree of certainty, with the understanding that exact site locations are subject to change; some sites may not be feasible to build due to regulatory, political or fiscal barriers; and some sites may be added to the initial conceptual design.				
MN-18	The service provider SHALL provide coverage maps depicting current coverage on an at least quarterly basis. The intent is for public safety agencies to include current coverage in their short-term communications planning efforts, including when to adopt the service.	N/A	SHALL		N/A
MN-19	The NPSBN SHALL provide neutral transport with a reasonable degree of Priority and QoS to all users on the NPSBN.	N/A	SHALL		N/A
MN-20	PSEs SHALL be able to manage encryption of traffic on the client side without modification or interruption to public safety traffic.	N/A	SHALL		N/A
MN-21	PSEs SHALL be able to manage their enterprise fleet the way they do today on commercial networks with enterprise-grade service.	N/A	SHALL		N/A
MN-22	Devices with the Apple iOS operating system SHALL be commercially available for use on the service.	N/A	SHALL		N/A
MN-23	Devices with the Stock Android operating system SHALL be commercially available for use on the service.	N/A	SHALL		N/A
MN-25	The service SHALL be competitively priced with cellular carrier services available in the state of Minnesota.	N/A	SHALL		N/A
MN-26	The service SHALL allow for 911 emergency calls to be made with parity to 911 calls placed over a commercial service.	N/A	SHALL		N/A
MN-27	The service SHALL provide carrier-grade voice telephony service.	N/A	SHALL		N/A
MN-30	The Minnesota Statewide Emergency Communications Board SHALL determine which agencies and users are allowed access to the NPSBN.	N/A	SHALL		N/A
MN-33	The service provider SHALL depict, in its coverage maps, whether access in that area is exclusive through Band 14, or if it is through other network services.	N/A	SHALL		N/A
MN-34	The service provider SHALL provide a single contract and Point-of-Contact for Band 14/NPSBN access AS WELL AS any roaming partners. The intent is that public safety agencies have a single service contract, and do not have multiple vendor service contracts to access the NPSBN and roaming partner networks.	N/A	SHALL		N/A
MN-35	The network operator SHALL provide detailed activity records for PSE users on an at least monthly basis. "Activity Records" includes at least the following: telephone call information, downlink data consumption, uplink data consumption, text/multimedia messages. Activity Records shall also include a breakdown of traffic through the NPSBN Band 14 network as opposed to roaming partner networks.	N/A	SHALL		N/A
MN-36	**FirstNet SHOULD establish a master contract with the state of Minnesota to make ordering devices and**	N/A	SHOULD	*See SOR 19.3.*	N/A

	service easier for end-user agencies.				
MN-37	**FirstNet SHOULD establish a master contract with US General Services Administration to make ordering devices and service easier for end-user agencies.**	N/A	SHOULD	*See SOR 19.3.*	N/A
SOR-1.1	FirstNet SHALL define the requirements for agencies and/or authorities to qualify as NPSBN users.	SHALL	SHALL NOT	*Minnesota's governance structure shall determine who defines the requirements to qualify as a user.*	Different
SOR-1.2	FirstNet SHOULD include any emergency response agency and/or authority with ESF responsibility as outlined in the NRF.	SHOULD	SHOULD		Same
SOR-2.1	FirstNet SHOULD collaboratively leverage existing statewide communication governance models to incorporate the input of the entire local, tribal, state, and federal community.	SHOULD	SHALL	*FirstNet is required to coordinate with the SECB under Minnesota statute. See MN Stat. 403.382 Subd. 8 Sec. 1: The SECB is responsible for developing and maintaining a plan for implementation of the NPSBN and to define technical and operational standards for the network.* *SECB and RECB/RESBs in Minnesota have substantial capability to support buy-in throughout the state at a highly granular level. The governance structure also provides an avenue to enforce compliance with standards and advocate for best practices, as well as to adopt standards and best practices with a high degree of stakeholder ownership.* *A coordinated governance structure across the state can manage conflicts regarding use of the network, abuse of network privileges and to coordinate special events across separate levels of government and with non-governmental user entities.* *Additionally, because RECB/RESBs are legal entities with the ability to enter into contracts and own property, they represent valid potential business partners or VMNO entities.*	Different
SOR-2.2	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.	SHOULD	SHALL WITH COMMENTS	*See comments and justification on 2.1.*	Different
SOR-3.1	FirstNet SHALL consult with tribal entities in the building, deployment, and operation of the NPSBN.	SHALL	SHALL		Same
SOR-3.2	FirstNet SHALL acknowledge and consider existing issues of tribal sovereignty and federal trust principles in the development of the NPSBN.	SHALL	SHALL		Same
SOR-4.1	FirstNet SHALL leverage the ECPC to effectively coordinate with federal agencies and to develop partnerships with federal agencies to support the	SHALL	SHALL		Same

	deployment, security, and operation of the NPSBN.				
SOR-4.2	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.	SHALL	SHALL		Same
SOR-5.1	FirstNet SHALL consider partnerships from the perspective of nationwide, local, tribal, multistate and federal entities and any relationships with industry partners.	SHALL	SHALL		Same
SOR-5.2	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.	SHALL	SHALL		Same
SOR-6.1	FirstNet SHALL develop a policy for the NPSBN that requires a nationwide standard for prioritization and QoS.	SHALL	SHALL		Same
SOR-6.2	FirstNet SHALL define the default priorities of all user classes on the NPSBN.	SHALL	SHALL		Same
SOR-6.3	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.	SHALL	SHALL		Same
SOR-6.4	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.	SHALL	SHALL WITH COMMENTS	*Devices workgroup voted to remove all "immediate peril" requirements.* *The network operator, except through special provisions of a roaming agreement, has no means to enforce or no reasonable expectation that a commercial carrier will preserve the priority classification of an emergency call.*	Different
SOR-6.5	The lowest network priorities SHALL be reserved for those users who lease the spectrum for commercial and/or personal use.	SHALL	SHALL		Same
SOR-7.1	FirstNet SHALL establish a policy to enable PSENs and PSEN applications to be accessed via the NPSBN.	SHALL	SHALL		Same
SOR-7.2	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.	SHALL	SHALL		Same
SOR-8.1	FirstNet administration SHALL establish an advisory body to assist PSE jurisdictions in migrating existing private wireless network data connectivity onto the NPSBN.	SHALL	SHALL		Same
SOR-9.1	FirstNet SHALL establish a certification process for all network hardware and firmware.	SHALL	SHALL		Same
SOR-9.2	FirstNet SHALL establish a policy to insure that all applicable components of the network comply with the Network Interoperability Certification Requirements.	SHALL	SHALL		Same
SOR-10.1	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.	SHALL	SHALL		Same
SOR-11.1	The NPSBN SHALL support future defined applications	SHALL	SHALL		Same

	as required by PS Users and as sanctioned by FirstNet.				
SOR-11.2	FirstNet SHALL implement a coverage and capacity expansion plan.	SHALL	SHALL WITH COMMENTS	*See Minnesota's Phased Buildout Strategy Requirements for FirstNet.*	Different
SOR-11.3	FirstNet SHALL implement process-improvement procedures for roadmap management including feature-request and feature-prioritization processes.	SHALL	SHALL		Same
SOR-12.1	FirstNet SHALL plan and maintain budget items for upgrades and technology refresh according to the established roadmap.	SHALL	SHALL		Same
SOR-12.2	FirstNet SHALL implement an upgrade/maintenance coordination and notification process with all appropriate partners.	SHALL	SHALL		Same
SOR-12.3	FirstNet SHALL maintain backwards compatibility with deployed UEs as allowed by 3GPP standards.	SHALL	SHALL		Same
SOR-12.4	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.	SHALL	SHALL		Same
SOR-13.1	FirstNet SHALL implement life-cycle management processes for interfaces exposed to applications, O&M Users, LTE Users, Non-LTE Users, and Network Administrators.	SHALL	SHALL		Same
SOR-14.1	FirstNet SHALL implement a coverage and capacity expansion plan.	SHALL	SHALL		Same
SOR-14.2	In conjunction with NPSBN service, a commercial cellular roaming agreement SHALL be offered.	SHALL	SHALL		Same
SOR-14.3	The NPSBN SHALL be capable of delivering a similar suite of features, functions, and capabilities as available over commercial cellular networks.	SHALL	SHALL		Same
SOR-14.4	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.	SHALL	SHALL		Same
SOR-14.5	A migration plan from the commercial cellular network to the NPSBN SHALL be developed in collaboration between Network Administrators and FirstNet.	SHALL	SHALL		Same
SOR-14.6	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.	SHALL	SHALL		Same
SOR-14.7	A commercial cellular system to NPSBN transition test plan SHALL be provided to assist migration to the NPSBN.	SHALL	SHALL		Same
SOR-15.1	FirstNet SHALL establish a policy to schedule network maintenance.	SHALL	SHALL		Same
SOR-15.2	FirstNet SHALL establish a policy to notify users of scheduled maintenance that may impact the user experience on the NPSBN.	SHALL	SHALL		Same
SOR-16.1	FirstNet SHALL develop policies regarding the billing of users and/or user agencies that reconcile usage by individual agencies and jurisdictions.	SHALL	SHALL		Same
SOR-16.2	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.	SHALL	SHALL		Same
SOR-17.1	FirstNet SHOULD develop a policy defining the ability and process for local, tribal, state, and federal entities to monitor the network.	SHOULD	SHOULD WITH COMMENTS	*SOR requirement does not define what "monitor" means and what is being monitored.*	Different
SOR-17.2	FirstNet SHALL establish policies to provide user entities prompt trouble reports, information helpful to facilitate operations using contingency	SHALL	SHALL WITH COMMENTS	*State Plan will detail SLA terms which will include trouble response.*	Different

	communications, and restoration reports.				
SOR-17.3	FirstNet SHALL establish a policy to provide user entities insight into overall system performance metrics, including availability and coverage.	SHALL	SHALL WITH COMMENTS	*State Plan will detail SLA terms which will include reporting required from the network operator.*	Different
SOR-18.1	FirstNet SHALL establish standardized training programs to deliver to all personnel who manage NPSBN communications resources.	SHALL	SHALL		Same
SOR-18.2	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.	SHALL	SHALL		Same
SOR-19.1	FirstNet SHALL implement policies and guidance to ensure **common NPSBN use and support.**	SHALL	SHALL WITH COMMENTS	*Workgroup assumes "common … use and support" means technical and operational standards for use and maintenance of the network.*	Different
SOR-19.2	FirstNet SHALL implement procedures for the activation, deployment, and deactivation of technical resources.	SHALL	SHALL WITH COMMENTS	*Workgroup assumes that "technical resources" means* ***both*** *technical staff (e.g., technicians dispatched to address network issues) as well as deployable equipment (e.g., COWs and cached UE).*	Different
SOR-19.3	FirstNet SHALL provide support for procurement of goods and services.	SHALL	SHALL WITH COMMENTS	*Most agencies in Minnesota currently order cellular services and devices off of state and GSA schedules.*	Different
SOR-19.4	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.	SHALL	SHALL		Same
SOR-20.1	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.	SHALL	SHALL		Same
SOR-20.2	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.	SHALL	SHALL		Same
SOR-21.1	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	SHOULD	SHOULD		Same

SOR-21.2	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).	SHALL	SHALL		Same
SOR-21.3	Encrypted NPSBN application content SHALL NOT be decrypted prior to transfer to the PSEN.	SHALL NOT	SHALL NOT		Same
SOR-21.4	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.	SHALL	SHALL		Same
SOR-21.5	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.	SHALL	SHALL WITH COMMENTS	*Note: Outside agencies or individuals may retrieve logging content either through public records requests or court order.*	Different
SOR-21.6	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.	SHALL	SHALL		Same
SOR-21.7	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).	SHALL	SHALL AS AMENDED	*SHALL include source/origination and destination identity (e.g., destination IP, user account, telephone #, etc. depending on the service being logged).*	Different
SOR-21.8	The NPSBN SHALL maintain logging usage records identifying which PSE O&M User activated or de-activated the logging service.	SHALL	SHALL WITH COMMENTS	*Assumes that O&M user **can** deactivate the logging service.*	Different
SOR-22.1	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.	SHALL	SHOULD	*Requirement assumes that FN is operating a centralized application distribution platform.* *This is not particularly important from an operational perspective.*	Different
SOR-22.2	Applications deployed by FirstNet SHALL support device addressing.	SHALL	SHALL		Same
SOR-22.3	Applications deployed by FirstNet SHALL support user addressing.	SHALL	SHALL		Same
SOR-22.4	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.	SHALL	SHALL		Same
SOR-22.5	For applications deployed by FirstNet, it SHALL be possible for the receiving NPSBN-U to identify the user	SHALL	SHALL		Same

	address of the content source. This requirement may not be readily achievable should the call or session originator be a non-NPSBN-U.				
SOR-22.6	For applications deployed by FirstNet, a common User Address format SHOULD be created. The intent is to define a consistent identification format.	SHOULD	SHALL	*Workgroup members feel that a common address format is **required**.*	Different
SOR-24.1	As identified in the previous table, FirstNet SHALL provide the identified user services to NPSBN-Us.	SHALL	SHALL		Same
SOR-24.2	As identified in the previous table, FirstNet SHALL enable PSE O&M Users to deploy the identified user services.	SHALL	SHALL		Same
SOR-24.3	FirstNet and the NPSBN SHALL NOT block or limit the capabilities of any user service deployed by the PSE O&M User.	SHALL NOT	SHALL NOT		Same
SOR-25.1	The NPSBN SHALL support full-duplex telephone sessions between a mobile NPSBN-U and the PSTN.	SHALL	SHALL		Same
SOR-25.2	The NPSBN SHALL support full-duplex telephone sessions between a mobile NPSBN-U and a commercial network user (CN-U).	SHALL	SHALL		Same
SOR-25.3	The NPSBN SHOULD support full-duplex telephone sessions to devices.	SHOULD	SHALL	*Workgroup assumes that "full-duplex" means "the telephone conversation appears to be full duplex to the user."*	Different
SOR-25.4	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.	SHALL	SHALL		Same
SOR-26.1	The NPSBN SHALL allow authorized PSE O&M Users (e.g., agency information technology staff) to configure which external networks the NPSBN-U can initiate telephony sessions with.	SHALL	SHALL		Same
SOR-26.2	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.	SHALL	SHALL		Same
SOR-26.3	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.	SHALL	SHALL		Same
SOR-26.4	The NPSBN SHALL allow authorized PSE O&M Users to optionally block anonymous or private incoming calls to their associated NPSBN-Us.	SHALL	SHALL		Same
SOR-27.1	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."	SHALL	SHALL		Same
SOR-27.2	The NPSBN SHALL allow authorized PSE O&M Users to	SHALL	SHALL		Same

	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.				
SOR-27.3	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."	SHOULD	SHOULD		Same
SOR-27.4	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.	SHALL	SHALL		Same
SOR-27.5	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.	SHALL	SHALL		Same
SOR-27.6	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.	SHALL	SHALL		Same
SOR-28.1	The NPSBN shall support the transmission of telephony caller addressing information (e.g., "Caller ID").	SHALL	SHALL		Same
SOR-28.11	It SHALL be possible for an authorized PSE O&M User to define an extension for an NPSBN-U or device.	SHALL	SHALL		Same
SOR-28.12	The telephone service SHALL support toll (or better) audio quality.	SHALL	SHALL		Same
SOR-28.2	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").	SHALL	SHALL		Same
SOR-28.3	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").	SHALL	SHALL		Same
SOR-28.4	The NPSBN shall support telephony voicemail service.	SHALL	SHALL		Same
SOR-28.5	On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the use of voicemail service.	SHALL	SHALL		Same
SOR-28.6	The voicemail service SHALL support a per-user passcode, which must be entered by the NPSBN-U prior to the management of voicemail message.	SHALL	SHALL		Same
SOR-28.7	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	SHALL	SHALL		Same
SOR-28.8	The NPSBN SHALL support telephony call conferencing.	SHALL	SHALL		Same

SOR-28.9	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.	SHALL	SHALL		Same
SOR-28.10	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).	SHALL	SHALL		Same
SOR-29.1	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.	SHALL	SHALL		Same
SOR-30.1	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.	SHALL	SHALL		Same
SOR-30.2	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.	SHALL	SHALL		Same
SOR-30.3	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.	SHALL	SHALL		Same
SOR-30.4	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.	SHALL	SHALL		Same
SOR-31.1	The NPSBN SHALL be able to receive CMAS alerts from the CMAS Federal Alert Gateway.	SHALL	SHALL		Same
SOR-31.2	The NPSBN SHALL support all three categories of CMAS alerts: Presidential, Imminent Threat, and Child Abduction/AMBER alerts.	SHALL	SHALL		Same
SOR-31.3	All NPSBN-U SHALL be able to receive CMAS text alerts using CMAS-capable UE that can present the alert.	SHALL	SHALL		Same
SOR-31.4	All NPSBN-Us SHALL be able to receive CMAS text alerts using CMAS-capable UE that can present the alert.	SHALL	SHALL		Same
SOR-31.5	NPSBN-Us SHOULD be allowed to opt-out of the presentation of specific alerts that are not Presidential alerts.	SHOULD	SHALL		Different
SOR-31.6	The NPSBN SHALL support the periodic testing of CMAS service as defined by the FCC.	SHALL	SHALL		Same
SOR-32.1	NPSBN-Us SHALL have the capability to send and receive text messages to and from other NPSBN-Us and CN-Us.	SHALL	SHALL		Same
SOR-32.2	NPSBN-Us SHALL have the capability to send text messages addressed to a group of NPSBN-Us.	SHALL	SHALL		Same
SOR-32.3	NPSBN-Us SHALL have the capability to send and receive multimedia messages to and from other NPSBN-Us.	SHALL	SHALL		Same
SOR-32.4	NPSBN-Us SHALL have the capability to send multimedia messages addressed to a group of NPSBN-Us.	SHALL	SHALL		Same
SOR-33.1	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	SHALL	SHALL		Same

	standard mechanism (e.g., SMTP) to allow for message interoperability with PSEN email systems as opposed to supporting many such interfaces.				
SOR-33.2	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 Pages13 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.	SHALL	SHALL		Same
SOR-33.3	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 Pages13 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.	SHALL	SHALL		Same
SOR-34.1	The NPSBN SHALL support the ability for a PSEN to deploy one or more video applications.	SHALL	SHALL		Same
SOR-34.2	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.	SHALL	SHALL		Same
SOR-34.3	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.	SHALL	SHALL		Same
SOR-35.1	The NPSBN SHALL provide the ability for one or more NPSBN-Us to stream video traffic in realtime to one or more other NPSBN-Us using the NSPBN video service.	SHALL	SHALL		Same
SOR-35.2	The NPSBN SHALL support the ability to interface with fixed video sources (including third-party systems), such as facility security cameras.	SHALL	SHALL		Same
SOR-36.1	The information content of NPSBN Status Web Pages SHALL be accessible for both reading and writing by applications.	SHALL	SHALL		Same
SOR-36.2	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.	SHALL	SHALL		Same
SOR-36.3	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.).	SHALL	SHALL		Same
SOR-36.4	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.	SHALL	SHALL		Same
SOR-37.1	The NPSBN SHOULD provide application hosting capabilities within the NPSBN.	SHOULD	SHOULD		Same
SOR-37.2	PSEs SHALL NOT be required to host applications within the NPSBN Services.	SHALL NOT	SHALL NOT		Same

SOR-37.3	PSEs SHALL be able to locally host applications within the agency PSEN.	SHALL	SHALL		Same
SOR-37.4	The NPSBN SHOULD provide a service hosting platform as a service to PSENs.	SHOULD	SHOULD		Same
SOR-37.5	The NPSBN SHALL provide the ability for PSEs to remotely manage their applications.	SHALL	SHALL		Same
SOR-37.6	The NPSBN SHOULD provide a service hosting platform as a service to vendors.	SHOULD	SHOULD		Same
SOR-37.7	The NPSBN SHALL provide the ability for vendors to remotely manage their applications.	SHALL	SHALL		Same
SOR-38.1	The NPSBN SHALL provide an application distribution and management service for NPSBN-U applications.	SHALL	SHALL		Same
SOR-39.1	The NPSBN SHALL provide the ability for UE devices to report location information to the network for device management and configuration purposes.	SHALL	SHALL		Same
SOR-39.11	The NPSBN presence service SHALL provide interface specifications for use by other application servers.	SHALL	SHALL		Same
SOR-39.2	The NPSBN SHALL limit access to UE device location information based on PSE policies.	SHALL	SHALL		Same
SOR-39.3	The NPSBN SHALL provide an application location service that stores UE locations tied to user ID for purposes of applications requiring locations.	SHALL	SHALL		Same
SOR-39.4	The information called Location Information SHOULD at a minimum include geographical location, time, date, and a unique identifier.	SHOULD	SHALL	*Workgroup assumes that "time" and "date" fields are the time and date that location was last updated for that individual.*	Different
SOR-39.5	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.	SHALL	SHALL		Same
SOR-39.6	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.	SHALL	SHALL		Same
SOR-39.7	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.	SHOULD	SHALL	*This should not preclude billing information (e.g., call log showing location at time of call).*	Different
SOR-39.8	The network management service SHALL allow an authorized entity to retrieve a particular UE's current network location (RAN, eNodeB).	SHALL	SHALL		Same
SOR-39.9	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.	SHALL	SHALL		Same
SOR-39.10	The NPSBN SHALL provide a presence service.	SHALL	SHALL		Same
SOR-40.1	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.	SHALL	SHALL		Same
SOR-40.2	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.	SHALL	SHALL		Same
SOR-40.3	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	SHALL	SHALL		Same

	emergency condition.				
SOR-41.1	The NPSBN SHALL provide the ability for the NPSBN-U (or other authorized user) to initiate and clear the Immediate Peril condition.	SHALL	SHALL NOT	*Workgroup deemed "immediate peril" was not a desired feature. Worse, it makes emergencies potentially more unsafe for responders.* *E.G., corrections. Man-down function--higher priority than other traffic.* *From dispatch perspective, the response to any emergency call would be the same. You have procedures to follow, and the content of the emergency call, and the response (or lack thereof) from the person initiating the emergency, determines the response to it.* *** Any "immediate peril" feature is to be a SHALL NOT on the basis that there should be only one emergency call function.*	Different
SOR-41.2	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.	SHALL	SHALL NOT	*Workgroup deemed "immediate peril" was not a desired feature. Worse, it makes emergencies potentially more unsafe for responders.*	Different
SOR-41.3	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.	SHALL	SHALL NOT	*Workgroup deemed "immediate peril" was not a desired feature. Worse, it makes emergencies potentially more unsafe for responders.*	Different
SOR-42.1	The NPSBN SHALL allow an NPSBN-U's priority and QoS to be altered dynamically based on the Incident and locally defined needs.	SHALL	SHALL NOT		Different
SOR-43.1	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.	SHALL	SHALL		Same
SOR-43.2	These DNS services, when provided, SHALL also be accessible from other public safety networks such as PSAPs.	SHALL	SHALL		Same
SOR-43.3	PSEs SHALL be actively notified of planned future changes in advance that may adversely affect their use of the network.	SHALL	SHALL		Same
SOR-43.4	PSEs SHOULD have a voice in approving DNS changes made to the NPSBN that have potential to adversely affect them.	SHOULD	SHOULD		Same
SOR-43.5	DNS services SHALL be deployed in such a manner to ensure resiliency, failover, ease of maintenance, and consistent high performance, and minimize backhaul traffic.	SHALL	SHALL		Same
SOR-43.6	To allow for nimble recovery from NSPBN system failures and ensure public safety users with a simple roaming experience, DNS server IP addresses SHOULD	SHOULD NOT	SHOULD NOT		Same

	NOT be hard coded in an individual UE.				
SOR-43.7	The NPSBN shall put in place a system to ensure IP addresses across the entire national level of the FirstNet system are unique.	SHALL	SHALL		Same
SOR-43.8	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.	SHALL	SHALL		Same
SOR-43.9	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.	SHALL	SHALL		Same
SOR-44.1	The NPSBN SHALL provide a network time service available to NPSBN infrastructure.	SHALL	SHALL		Same
SOR-44.2	The NPSBN SHALL provide a network time service available to mobile users of the network.	SHALL	SHALL		Same
SOR-45.1	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.	SHOULD	SHOULD NOT	*There is limited value in FN developing an NPSBN-specific application delivery platform when device vendors and PSENs operate these platforms today.*	Different
SOR-46.1	The identity management framework SHALL enable applications and services to securely verify the identity of users.	SHALL	SHALL		Same
SOR-46.2	The identity management framework SHALL be standards based.	SHALL	SHALL		Same
SOR-46.3	Identity assertions SHALL be cryptographically protected when being transmitted from one entity to another in the network.	SHALL	SHALL		Same
SOR-46.4	The identity management framework SHALL issue identities to non-person entities on the network.	SHALL	SHALL		Same
SOR-46.5	The identity management framework SHALL enable non-person entities to authenticate to applications and services where authorized.	SHALL	SHALL		Same
SOR-46.6	The NPSBN SHALL define the process and procedures necessary for organizations (local, tribal, state, and federal) to gain approval to join the trust framework.	SHALL	SHALL		Same
SOR-47.1	Governance of individual digital user identities SHALL be maintained by the local, tribal, state, or federal organization from which the user is affiliated.	SHALL	SHALL		Same
SOR-47.2	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.	SHALL	SHALL		Same
SOR-48.1	NPSBN devices SHOULD be capable of being shared amongst different authorized human users.	SHOULD	SHALL	*Workgroup assumes that if this requirement applies to devices with a human interface, e.g., smartphones and tablets; this requirement applies by default to devices without a human interface, e.g., router or hotspot.* *Regardless of the authentication scheme deployed by FirstNet, there is no real physical limitation preventing multiple individuals from sharing a device.* *The authentication of individual human users is an individual agency issue, per varying federal,*	Different

				state, and local laws and standards; FN shall not apply an additional layer of user authentication as a prerequisite for a device accessing the NPSBN. *CJIS requires unique authentication requirements for individual users.*	
SOR-49.1	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.	SHALL	SHALL		Same
SOR-49.2	The NPSBN SHALL have access to the identity management framework for purposes of user activity monitoring, security monitoring, and application delivery.	SHALL	SHALL		Same
SOR-49.3	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.	SHALL	SHALL		Same
SOR-49.4	The NPSBN authentication services SHALL support industry standard authentication interfaces for mobile and fixed infrastructure components.	SHALL	SHALL		Same
SOR-50.1	The identity management framework SHALL manage privileges for person and non-person entities.	SHALL	SHALL		Same
SOR-50.2	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.	SHALL	SHALL		Same
SOR-52.1	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.	SHALL	SHALL		Same
SOR-52.2	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.	SHALL	SHALL		Same
SOR-52.3	The device management network service SHALL allow an authorized entity to configure a UE to be able to access one or more wireless networks.	SHALL	SHALL		Same
SOR-52.4	The NPSBN SHALL support Over-the-Air (OTA) SIM management.	SHALL	SHALL		Same
SOR-52.5	The NPSBN SHALL support OTA Firmware Update management.	SHALL	SHALL		Same
SOR-52.6	The NPSBN SHALL support OTA Software Configuration management.	SHALL	SHALL		Same
SOR-52.7	The NPSBN SHALL support OTA APN connection management.	SHALL	SHALL		Same
SOR-52.8	The NPSBN SHALL support OTA Diagnostics Monitor (e.g., LTE radio statistics) management.	SHALL	SHALL		Same
SOR-53.10	The NPSBN architecture SHALL provide transport between CMAS and a NPSBN-U.	SHALL	SHALL		Same
SOR-53.10	The NPSBN architecture SHALL provide transport between a NPSBN-U and its home PSEN.	SHALL	SHALL		Same
SOR-53.11	The NPSBN architecture SHALL provide transport between NPSBN Services and a PSEN.	SHALL	SHALL		Same
SOR-53.12	The NPSBN architecture SHALL provide transport between NPSBN Services and NPSBN O&M Services.	SHALL	SHALL		Same
SOR-53.13	The NPSBN architecture SHALL provide transport between NPSBN Services and 9-1-1call centers.	SHALL	SHALL		Same
SOR-53.14	The NPSBN architecture SHALL provide transport	SHALL	SHALL		Same

	between NPSBN Services and the PSTN. (This is required if PSTN service is implemented at launch.)				
SOR-53.15	The NPSBN architecture SHALL provide transport between NPSBN O&M Services and a PSEN.	SHALL	SHALL		Same
SOR-53.16	The NPSBN architecture SHALL provide transport between a PSEN and commercial networks.	SHALL	SHALL		Same
SOR-53.17	The NPSBN architecture SHALL provide transport between a PSEN and a NPSBN EPC.	SHALL	SHALL		Same
SOR-53.18	The NPSBN architecture SHALL provide transport between NPSBN O&M Services and a NPSBN EPC.	SHALL	SHALL		Same
SOR-53.2	The NPSBN architecture SHALL provide transport between a NPSBN-U and non-home PSEN as needed.	SHALL	SHALL		Same
SOR-53.3	The NPSBN architecture SHALL provide transport between a NPSBN-U and the PSTN. (This is required if PSTN service is implemented at launch.)	SHALL	SHALL		Same
SOR-53.4	The NPSBN architecture SHALL provide transport between a NPSBN-U and NPSBN Services.	SHALL	SHALL		Same
SOR-53.5	The NPSBN architecture SHALL provide transport between a NPSBN-U and NPSBN O&M Services.	SHALL	SHALL		Same
SOR-53.6	The NPSBN architecture SHALL provide transport between a NPSBN-U and 9-1-1call centers.	SHALL	SHALL		Same
SOR-53.7	The NPSBN architecture SHALL provide transport between a NPSBN-U and another NPSBN-U attached to the same EPC.	SHALL	SHALL		Same
SOR-53.8	The NPSBN architecture SHALL provide transport between a NPSBN-U and another NPSBN-U attached to a different EPC.	SHALL	SHALL		Same
SOR-53.9	The NPSBN architecture SHALL provide transport between a NPSBN-U and a commercial roaming exchange.	SHALL	SHALL		Same
SOR-54.1	The nationwide private IP network SHALL support route diversity to provide public-safety grade reliability.	SHALL	SHALL		Same
SOR-54.2	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.	SHALL	SHALL		Same
SOR-54.3	The nationwide private IP network SHALL support power backup for public safety-grade level of continuous electricity outage.	SHALL	SHALL		Same
SOR-55.1	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).	SHALL	SHALL		Same
SOR-55.2	Agencies' PSEN SHALL be allowed to connect to the NPSBN through the Internet and not be required to support a physical connection.	SHALL	SHALL		Same
SOR-56.1	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).	SHALL	SHALL		Same
SOR-56.2	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)	SHALL	SHALL		Same
SOR-56.3	The nationwide private IP network SHALL provide enough bandwidth to support the capacity necessary for the user's applications that are connected.	SHALL	SHALL		Same
SOR-57.1	The NPSBN SHALL support an agency's ability to perform a secondary authentication before allowing an NPSBN-U to connect with a PSEN.	SHALL	SHALL		Same
SOR-57.2	The NPSBN SHALL support a communication path	SHALL	SHALL		Same

	between an agency's NPSBN-U's and the PSEN without imposing a NAT.				
SOR-57.3	The NPSBN SHALL support local IP applications in the PSEN.4	SHALL	SHALL		Same
SOR-57.4	The NPSBN SHALL support transport of VPN traffic from an NPSBN-U to the PSEN.	SHALL	SHALL		Same
SOR-57.5	The NPSBN SHALL support transport of prioritized traffic from/to the PSEN.	SHALL	SHALL		Same
SOR-58.1	NPSBN services SHALL be accessible directly from a NPSBN-U connected to the NPSBN by an authorized user.	SHALL	SHALL		Same
SOR-58.2	NPSBN services SHALL be accessible directly from a NPSBN-U connected to a commercial or other network by an authorized user.	SHALL	SHALL		Same
SOR-58.3	FirstNet SHALL size the connections to each PSEN in accordance with the SLA with the PSEN.	SHALL	SHALL		Same
SOR-58.4	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.	SHALL	SHALL		Same
SOR-58.5	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.	SHALL	SHALL		Same
SOR-58.6	NPBSN services SHALL be accessible from a PSEN by authorized users connected to the PSEN via any means.	SHALL	SHALL		Same
SOR-58.7	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.	SHALL	SHALL		Same
SOR-59.1	The NPSBN and NPSBN-U equipment SHALL support NPSBN-U mobility across the entire NPSBN.	SHALL	SHALL		Same
SOR-59.2	The NPSBN and NPSBN-U equipment SHALL support NPSBN-U roaming from the NPSBN to commercial networks as per established roaming agreements.	SHALL	SHALL		Same
SOR-59.3	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.	SHALL	SHALL		Same
SOR-59.4	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.	SHALL	SHALL		Same
SOR-60.1	NPSBN-U SHALL have access to the Internet via NPSBN transport to access any Internet provided service or data.	SHALL	SHALL		Same
SOR-60.2	The NPSBN SHALL allow VPN access to data via the Internet transport.	SHALL	SHALL		Same
SOR-60.3	The NPSBN SHALL be protected against attack via the Internet access and PSEN's shall follow FirstNet security policies.	SHALL	SHALL		Same
SOR-60.4	User agencies SHALL have the option to block Internet access to their user devices.	SHALL	SHALL		Same
SOR-60.5	User agencies SHALL have the option to provide Internet access to their devices via their own agency Internet transport.	SHALL	SHALL		Same

SOR-61.1	The NPSBN SHALL guarantee a level of accessibility and retainability of critical services across FirstNet's service area throughout the different deployment phases.	SHALL	SHALL	*Pending contents of State Plan from FirstNet as negotiated by Minnesota and FirstNet; also pending Phased buildout milestones from Minnesota.*	Same
SOR-61.11	Intra-NPSBN handover SHALL NOT be perceptible to the user.	SHALL NOT	SHALL NOT		Same
SOR-61.12	The use of standard-compliant high-power NPSBN UEs SHALL NOT create harmful interference to any UEs' NPSBN services.	SHALL NOT	SHALL NOT WITH COMMENTS	*All NPSBN devices should conform to 3GPP power control specs, so from a technical perspective, this should not be an issue.* *Also, the FCC will not likely type-certify cellular devices that will cause harmful interference.*	Different
SOR-61.13	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).	SHALL NOT	SHALL NOT		Same
SOR-61.2	The NPSBN SHALL be designed according to measurable GoS levels throughout the NPSBN service area.	SHALL	SHALL		Same
SOR-61.3	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).	SHALL	SHALL		Same
SOR-61.4	The required data throughput performance of applications SHALL be maintained at vehicular speeds.	SHALL	SHALL		Same
SOR-61.5	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.	SHALL NOT	SHALL NOT		Same
SOR-61.6	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.	SHALL	SHALL		Same
SOR-61.7	To ensure a reasonable end-to-end quality of service, performance level benchmarks SHOULD be included in roaming agreements between FirstNet and commercial carriers.	SHOULD	SHALL	*Workgroup finds it highly unlikely that FirstNet would enter into a roaming agreement without an agreed-upon performance level benchmark, even if that benchmark is "best effort".* *Workgroup members also feel their agencies would need to know the level of service when roaming off of FirstNet, as opposed being a regular customer of that roaming partner, much as they would today when assessing a VNMO entity.*	Different
SOR-61.8	The NPSBN SHALL be engineered to prevent traffic congestion at every stage of the network to meet the NPSBN GoS objectives.	SHALL	SHALL		Same
SOR-61.9	The NPSBN SHALL support capacity and/or coverage expansion to address evolving users' needs.	SHALL	SHALL		Same
SOR-61.10	The design of the NPSBN SHALL account for higher traffic demand in areas deemed strategic by FirstNet and/or PSEs.	SHALL	SHALL		Same

SOR-62.1	FirstNet SHALL provide coverage in the service area(s) required by PSE.	SHALL	SHALL		Same
SOR-62.2	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.	SHALL	SHALL	*See specific coverage objectives articulated by Minnesota as part of MnFCP.*	Same
SOR-62.3	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/nonurban, indoor/outdoor, portable/vehicular) and region(s) specific to the PSE.	SHALL	SHALL	*Can we measure per user? Hard to do because number of users changes the throughput per user. PCRF configuration determines bandwidth available.* *User expectation will be comparable either to current radio systems or to ARMER. ARMER provides guaranteed minimum 95% geographic coverage with 4 voice channels to a mobile antenna on a county-by-county basis. In reality, in almost all cases the coverage is much better than the guaranteed minimum.*	Same
SOR-62.4	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.	SHALL	SHALL		Same
SOR-62.5	Coverage validation SHALL follow industry “best” practices.	SHALL	SHALL		Same
SOR-62.6	The RF planning and design of the NPSBN SHALL account for the possible coexistence of standard-compliant low and high-power UEs.	SHALL	SHALL		Same
SOR-63.1	The NPSBN infrastructure's availability SHALL be typical of a public-safety grade network.	SHALL	SHALL		Same
SOR-63.2	Issues impacting availability SHALL be managed within agreed SLAs.	SHALL	SHALL		Same
SOR-64.1	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.	SHALL	SHALL		Same
SOR-64.2	Service restoration time following an outage SHALL be minimal as per a service level agreement.	SHALL	SHALL		Same
SOR-64.3	Scheduled maintenance SHALL have minimal impact on services.	SHALL	SHALL		Same
SOR-64.4	Silent failure modes, i.e., failed backup components that have gone undetected, SHALL be minimized.	SHALL	SHALL		Same
SOR-64.5	The network SHALL revert to its original state of operation upon failure resolution.	SHALL	SHALL		Same
SOR-64.6	Adequate spare parts, antennas, transmission lines SHALL be stocked by the servicing agency.	SHALL	SHALL		Same
SOR-64.7	Remote reset of RAN equipment SHALL be available at each site.	SHALL	SHALL		Same
SOR-64.8	Any redundant NPSBN core SHALL support the full RAN traffic load.	SHALL	SHALL		Same
SOR-64.9	Shelters housing NPSBN equipment SHALL be hardened according to best practices employed in the region.	SHALL	SHALL		Same
SOR-64.10	The design of the NPSBN SHALL account for the following: Electromagnetic Interference (EMI), lightning protection, power surge protection, and tower wind loading.	SHALL	SHALL		Same

SOR-65.1	Backhaul links SHALL be designed for high availability.	SHALL	SHALL		Same
SOR-65.2	Design of the backhaul SHALL account for traffic overloads, e.g., during large-scale events.	SHALL	SHALL		Same
SOR-65.3	Backhaul links SHOULD be engineered to distinguish (or segregate between) PSEN traffic from (and) secondary users traffic when applicable.	SHOULD	SHALL	*Highway patrol: concept of system is that public safety entities will be provided priority traffic throughout.* *Priority/pre-emption should not apply only at the RAN but throughout the network's QoS configuration.* *Re conference at Boulder: If a secondary user is activated as a first responder they should be afforded the same level of priority as a normal priority user.* *What is a "secondary user"?*	Different
SOR-65.4	Backhaul transmission delays SHALL support the end-to-end delay budgets established for latency-sensitive applications.	SHALL	SHALL		Same
SOR-65.5	Switchover time from a primary path to a redundant path SHALL be imperceptible to LTE-users.	SHALL	SHALL		Same
SOR-65.6	All backhaul and inter-connect sites SHALL be protected against loss of commercial power.	SHALL	SHALL		Same
SOR-65.7	Secure remote monitoring, configuration, troubleshooting, and reset of transport equipment SHALL be available at each node.	SHALL	SHALL		Same
SOR-65.8	The backhaul network SHALL be scalable to accommodate traffic growth.	SHALL	SHALL		Same
SOR-66.1	NPSBN-Us SHOULD have consumer-equivalent smartphones capable of operating on both commercial networks and the NPSBN.	SHOULD	SHALL	*Workgroup members feel there is very little interest in a service that does not provide consumer-equivalent devices.*	Different
SOR-66.2	NPSBN-Us SHOULD have consumer-equivalent tablet PCs capable of operating on both commercial networks and the NPSBN.	SHOULD	SHALL	*Workgroup members feel there is very little interest in a service that does not provide consumer-equivalent devices.*	Different
SOR-66.3	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.	SHOULD	SHALL	*Workgroup members feel there is very little interest in a service that does not provide consumer-equivalent devices.*	Different
SOR-66.4	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).	SHOULD	SHALL	*Workgroup members feel there is very little interest in a service that does not provide consumer-equivalent devices.*	Different
SOR-67.1	NPSBN UE device SHALL provide a clear indication to the NPSBN-U when the UE device is roaming (not using the NPSBN).	SHALL	SHALL		Same
SOR-67.2	NPSBN UE SHALL support dual stack IPv4/IPv6.	SHALL	SHALL		Same
SOR-67.3	NPSBN UE SHOULD support enhanced autonomous location services (e.g., latitude, longitude).	SHOULD	SHALL	*Location services are **required**, not requested.*	Different
SOR-67.4	NSPBN UE SHOULD operate at power levels to meet the NPSBN coverage needs.	SHOULD	SHALL	*As 3GPP standards supporting high-power devices and commercial availability of the devices allows.*	Different
SOR-68.1	The NPSBN-U SHALL have UEs that support FirstNet-approved minimum set of voice and video CODECs.	SHALL	SHALL		Same
SOR-69.1	The NPSBN O&M solution SHALL provide provisioning and management of NPSBN Users (NPSBN-U).	SHALL	SHALL		Same
SOR-69.2	The NPSBN O&M solution SHALL provide access to	SHALL	SHALL		Same

	detailed, current, and historical billing and usage information per Section 4.6.9.				
SOR-70.1	The NPSBN SHALL have the ability provide an alarm stream to each PSE, scoped to network/service outage-level events.	SHALL	SHALL		Same
SOR-71.1	The NPSBN SHALL provide a secure performance management interface scoped to the PSE.	SHALL	SHALL		Same
SOR-71.2	The NPSBN SHALL provide performance data scoped to the PSE.	SHALL	SHALL		Same
SOR-71.3	The NPSBN SHALL provide an O&M tool interface to the NPSBN performance management system secured with the appropriate authentication and authorization controls.	SHALL	SHALL		Same
SOR-72.1	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).	SHALL	SHALL		Same
SOR-72.2	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.	SHALL	SHALL		Same
SOR-72.3	The User setup interface SHALL allow for an API interface that will process TXT, CSV, or XML files to facilitate bulk provisioning.	SHALL	SHALL		Same
SOR-73.1	Each PSE administrator SHALL have the ability to define the types of devices the user is authorized to use.	SHALL	SHALL		Same
SOR-73.2	Each PSE administrator SHALL have the ability to remove the assignment of certain types of devices the user is authorized to use.	SHALL	SHALL		Same
SOR-73.3	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.	SHOULD	SHOULD		Same
SOR-73.4	The user setup interface SHALL allow for an API that will process TXT, CSV, or XML files to facilitate bulk provisioning.	SHALL	SHOULD	*Per SOR, applies to setup of devices. Bulk provisioning would be a useful feature, but it is not available with carrier enterprise services today, and so as a minimum barrier to adoption it is not required.*	Different
SOR-74.1	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).	SHALL	SHALL		Same
SOR-74.2	Each PSE administrator SHALL have the ability to change the authorized applications and their settings.	SHALL	SHALL		Same
SOR-74.3	Each PSE administrator SHALL have the ability to remove the authorization to access an application.	SHALL	SHALL		Same
SOR-74.4	The user setup interface SHALL allow for an API that will process TXT, CSV, or XML files to facilitate bulk provisioning.	SHALL	SHALL		Same
SOR-75.1	Each PSE administrator SHALL have the ability to create new problem tickets related to the user device, and application setup process.	SHALL	SHALL		Same
SOR-75.2	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.	SHALL	SHALL		Same
SOR-75.3	Each PSE administrator SHALL have access to summary	SHALL	SHALL		Same

	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.				
SOR-76.1	Each PSE administrator SHALL have the ability to record in inventory, assign, and track devices in the local replacement pool.	SHALL	SHALL		Same
SOR-76.2	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.	SHALL	SHALL		Same
SOR-77.1	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.	SHALL	SHALL		Same
SOR-77.2	Each PSE administrator SHOULD have the ability to reset individual users to the pre-incident setting in a one-step action.	SHOULD	SHOULD		Same
SOR-78.1	The NPSBN SHALL provide an O&M tool.	SHALL	SHALL		Same
SOR-79.1	The NPSBN Billing Interface SHALL supply user, device, and application billing information in PDF and open standards formats (CSV, XML, TAP3, etc.).	SHALL	SHALL		Same
SOR-79.2	The NPSBN Billing Interface SHALL reconcile all billing activity with its commercial carrier partners and national public safety applications on behalf of the PSEs.	SHALL	SHALL		Same
SOR-79.3	PSE SHALL have access to transactions for their activity at the level equivalent CDRs but in a uniform, vendor-neutral format.	SHALL	SHALL		Same
SOR-79.4	The NPSBN Billing Interface SHALL provide sufficient billing detail for transport, multicarrier roaming, and application level usage to allow local administrator invoice validation.	SHALL	SHALL		Same
SOR-79.5	The NPSBN Billing Interface SHALL provide commercial and application level integration capability.	SHALL	SHALL		Same
SOR-79.6	The NPSBN Billing Interface SHALL supply an interface for PSEs to query up-to-date billing detail at will.	SHALL	SHALL		Same
SOR-80.1	A PSE O&M administrator SHALL have the ability to add devices quickly and efficiently without coordination with others.	SHALL	SHALL		Same
SOR-80.2	A PSE O&M administrator SHALL have the ability to configure the device remotely.	SHALL	SHALL		Same
SOR-80.3	A PSE O&M administrator SHALL have the ability to push software upgrades/updates.	SHALL	SHALL		Same
SOR-80.4	A PSE O&M administrator SHALL have the ability to install additional applications.	SHALL	SHALL		Same
SOR-80.5	A PSE O&M administrator SHALL have the ability to control access to the device.	SHALL	SHALL		Same
SOR-80.6	A PSE O&M administrator SHALL have the ability to authenticate users.	SHALL	SHALL		Same
SOR-80.7	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).	SHALL	SHALL		Same
SOR-80.8	A PSE O&M administrator SHALL have the ability to remove applications and/or deactivate device applications.	SHALL	SHALL		Same
SOR-81.1	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to download software, web links, and/or shortcuts to the device.	SHALL	SHALL		Same
SOR-81.2	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to set passwords and other security features on their device.	SHALL	SHALL		Same

SOR-81.3	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to enable Wi-Fi and Bluetooth features as required.	SHALL	SHALL		Same
SOR-82.1	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.	SHALL	SHALL		Same
SOR-83.1	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.	SHALL	SHALL		Same
SOR-84.1	The RAN, EPC, and transport equipment SHALL support capacity expansion of existing equipment or addition of new elements while minimizing out-of-service time.	SHALL	SHALL		Same
SOR-85.1	The RAN, EPC, and transport equipment SHALL support capabilities to add redundant components while minimizing out-of-service time.	SHALL	SHALL		Same
SOR-86.1	The NPSBN location service SHALL provide location information associated with NPSBN users.	SHALL	SHALL		Same
SOR-86.2	The NPSBN location service SHALL support authorization for access to NPSBN users' location information.	SHALL	SHALL		Same
SOR-86.3	NPSBN-U location information SHALL be available to PSEN hosted applications	SHALL	SHALL		Same
SOR-86.4	NPSBN-U location information SHALL be available to applications hosted via NPSBN Services.	SHALL	SHALL		Same
SOR-86.5	The NPSBN location service SHALL support strong security between location clients and servers.	SHALL	SHALL		Same
SOR-86.6	The NPSBN location service SHALL support receiving location information from NPSBN users while roaming.	SHALL	SHALL		Same
SOR-87.1	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.	SHALL	SHALL		Same
SOR-87.2	FirstNet SHALL define an NPSBN security policy for monitoring, logging, and data retention policies for NPSBN applications and services.	SHALL	SHALL		Same
SOR-88.1	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.	SHALL	SHALL		Same
SOR-88.2	FirstNet SHALL define a policy to insure that updates to security management will not compromise existing security measures.	SHALL	SHALL		Same
SOR-88.3	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.	SHALL	SHALL		Same
SOR-88.4	The RAN, EPC, and transport equipment SHALL support capabilities to respond, in near real-time, to security threats.	SHALL	SHALL		Same
SOR-88.5	Updates to security management SHALLNOT compromise existing security measures.	SHALL	SHALL		Same
SOR-89.1	Applications hosted on the NPSBN SHALL comply with all NPSBN information assurance procedures, policies, and requirements.	SHALL	SHALL		Same
SOR-89.2	PSEs SHALL be allowed to provide additional layers of security if desired.	SHALL	SHALL		Same
SOR-89.3	FirstNet's security policy for user services and NPSBN-hosted applications SHALL require users to securely authenticate for access.	SHALL	SHALL		Same

SOR-89.4	FirstNet’s security policy for user services and NPSBN-hosted applications SHALL provide and maintain anti-malware and anti-virus protection.	SHALL	SHALL		Same
SOR-89.5	FirstNet’s security policy SHALL require applications and user services to be secure against intrusion.	SHALL	SHALL		Same
SOR-89.6	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.	SHALL	SHALL WITH COMMENTS	*Public safety agencies are highly likely to comply with a wide variety of security polices already, and it is unlikely that any unique FN security policy would be burdensome to a PSE.*	Different
SOR-90.1	The NPSBN SHALL protect user services infrastructure to ensure localities, regions, or the nationwide services are not impacted by various cyber-attacks scenarios.	SHALL	SHALL		Same
SOR-90.2	The NPSBN SHALL protect user services infrastructure against corruption or unauthorized modification (e.g., software, configurations, etc.).	SHALL	SHALL		Same
SOR-90.3	The NPSBPN SHALL periodically verify that the user services infrastructure and hosted applications servers do not present security vulnerabilities.	SHALL	SHALL		Same
SOR-90.4	NPSBN user services SHALL meet public safety-grade availability and reliability requirements.	SHALL	SHALL		Same
SOR-91.1	The NPSBN SHALL provide user services and applications hosted on the NPSBN access to the NPSBN identity management framework.	SHALL	SHALL		Same
SOR-91.2	NPSBN user services and applications SHALL use the NPSBN identity management system.	SHALL	SHALL		Same
SOR-91.3	NPSBN-hosted agency applications SHALL use the NPSBN identity management system.	SHALL	SHOULD	*Workgroup finds this requirement from NPSTC SOR to be too speculative to necessitate a firm "SHALL" requirement. However, assuming FirstNet does offer a hosting environment for PSENs, this is probably a best practice.*	Different
SOR-91.4	PSEN-hosted applications SHALL be allowed to use the NPSBN identity management system.	SHALL	SHALL		Same
SOR-91.5	PSEN-hosted applications SHALL NOT be required to use the NPSBN identity management system.	SHALL NOT	SHALL NOT		Same
SOR-91.6	The NPSBN SHALL permit the use of last-used credentials to allow the setup of emergency calls without due course to the usual authentication process.	SHALL	SHALL NOT	*If a unit is decommissioned; it SHALL NOT retain any identifying information used for public PSE users including a PSE user's telephone number.* *We need to positively and uniquely who the user and device are.* *Note: "Emergency call" means "a call placed while the user is in an emergency condition".*	Different
SOR-92.1	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.	SHALL	SHALL		Same
SOR-92.2	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.	SHALL	SHALL		Same
SOR-92.3	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).	SHALL	SHALL		Same

SOR-92.4	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.	SHALL	SHALL		Same
SOR-92.5	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.	SHALL	SHALL		Same
SOR-93.1	NPSBN-Us SHALL be authenticated prior to accessing the text and multimedia messaging service.	SHALL	SHALL		Same
SOR-93.2	NPSBN-Us SHALL be suitably authorized prior to accessing the text and multimedia messaging service.	SHALL	SHALL		Same
SOR-93.3	The messaging service SHALL provide confidentiality for text and multimedia messaging (both message content and related control).	SHALL	SHALL		Same
SOR-93.4	The NPSBN SHALL provide the capability to filter spam and other undesirable text and multimedia messages as per configured policy.	SHALL	SHALL		Same
SOR-93.5	The NPSBN SHALL provide the capability to detect text and multimedia messaging infected with malware and prevent its delivery to the intended target.	SHALL	SHALL		Same
SOR-93.6	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.	SHALL	SHALL		Same
SOR-93.7	The messaging service SHALL have the ability to “whitelist” messaging contacts.	SHALL	SHALL		Same
SOR-93.8	The messaging service SHALL have the ability to “blacklist” messaging contacts.	SHALL	SHALL		Same
SOR-93.9	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.	SHALL	SHALL		Same
SOR-94.1	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.	SHALL	SHALL		Same
SOR-94.2	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.	SHALL	SHALL		Same
SOR-95.1	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.	SHALL	SHALL		Same
SOR-95.2	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.	SHALL	SHALL	*Workgroup notes that the policy for determining that a site, application, data type or address is malicious and the specific tools used to filter or block traffic are very important governance issues.*	Same
SOR-95.3	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	SHOULD	SHOULD		Same

	boundary device is between.				
SOR-95.4	The NPSBN SHALL have the ability to alert any PSENs, NPSBN-Us, or PSEs of illegal, inappropriate, or problematic boundary activities.	SHALL	SHALL		Same
SOR-96.1	The NPSBN SHALL monitor all common infrastructure components, servers, routers, gateways, and other vulnerable equipment using appropriate malware and virus protection mechanisms.	SHALL	SHALL		Same
SOR-96.2	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.	SHALL	SHALL		Same
SOR-96.3	The NPSBN SHALL provide protection of any shared services applications to assure they are safe from malware, virus, and zero day infestations.	SHALL	SHALL		Same
SOR-97.1	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.	SHALL	SHALL		Same
SOR-97.2	The NPSBN SHALL consider all UEs as untrusted and shall enforce security policies that protect NPSBN assets from UEs.	SHALL	SHALL		Same
SOR-97.3	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.	SHALL	SHALL		Same
SOR-97.4	The NPSBN SHOULD notify the appropriate agency or locality of any rogue device or devices deemed improper allocated to that agency PSEN.	SHOULD	SHOULD		Same
SOR-98.1	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.	SHALL	SHALL		Same
SOR-98.2	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.	SHALL	SHALL		Same
SOR-98.3	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.	SHALL	SHALL		Same
SOR-98.4	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.	SHALL	SHALL WITH COMMENTS	*Workgroup feels that a scenario requirement that the NPSBN exercise this feature is very unlikely, but it is a critical feature in the event that an access point is compromised.*	Different
SOR-99.1	The NPSBN SHALL store and monitor access logs that provide information on the identity of access devices, agency, role, and location.	SHALL	SHALL		Same
SOR-99.2	Access to the stored data SHALL be limited on a need-to-know basis and within the proper access rules dictated by policy.	SHALL	SHALL		Same
SOR-99.3	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.	SHALL	SHALL		Same
SOR-99.4	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	SHALL	SHALL		Same

	to support post-event activities.				
SOR-100.1	The NPSBN SHALL support access controls necessary to limit users from access to network control and signaling assets.	SHALL	SHALL		Same
SOR-100.2	The NPSBN SHALL support the ability based on a user's identity to limit or expand access to either shared or private services served locally, regionally, or nationwide including other PSENs.	SHALL	SHALL		Same
SOR-100.4	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.	SHALL	SHALL		Same
SOR-100.5	The NPSBN SHALL have the ability to shut off access of rogue or lost devices, or any other device according to policy.	SHALL	SHALL		Same
SOR-100.6	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.	SHALL	SHALL		Same
SOR-101.1	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.	SHALL	SHALL	*Most agencies are likely to manage their networks and security, including credentials and certificates, independently.* *Implies that FirstNet-deployed applications may require that the user is on a FirstNet VPN; in that case, both parties will have to support split tunneling.*	Same
SOR-101.3	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.	SHALL	SHALL		Same
SOR-101.4	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.	SHALL	SHALL		Same
SOR-102.1	The NPSBN SHALL protect using encryption and access control the network signaling, configuration, and other control interfaces of the network.	SHALL	SHALL		Same
SOR-102.2	The NPSBN SHALL limit access by user, function, and on a need-to-know basis to network control components.	SHALL	SHALL		Same
SOR-102.3	The NPSBN SHALL log and monitor all network control and signaling activities, and alerts will be generated when improper activity is detected.	SHALL	SHALL		Same
SOR-102.4	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.	SHOULD	SHALL	*Workgroup member agencies have background check/security clearance requirements for elevated access to their own networks, and expect no less from the NPSBN.*	Different
SOR-103.1	The NPSBN SHALL consider all independent agency networks as untrusted interfaces unless otherwise certified as trusted zones and agreed upon between agencies.	SHALL	SHALL		Same
SOR-103.2	The NPSBN SHALL provide firewall, IDS, and other cyber security protection devices at the interface points where untrusted network interfaces connect to the network.	SHALL	SHALL		Same
SOR-103.3	The NPSBN SHALL provide sensor data from the deployed sensor devices to the Security Operations for threat and operational analysis and response.	SHALL	SHALL		Same
SOR-103.4	The NPSBN SHALL have the ability to shut down any	SHALL	SHALL		Same

	external interface or connection to roaming network if security threats are detected and determined to be a threat to NPSBN operations.				
SOR-104.1	NPSBN UE SHALL be compliant with the security requirements of the Network Services, User Service, and Transport sections of this specification.	SHALL	SHALL		Same
SOR-104.2	NPSBN-Us SHOULD require UEs that can be completely disabled remotely (i.e., “kill”) when compromised.	SHOULD	SHALL	*This is a service available to agencies today through enterprise services with cellular carriers, and workgroup members expect no less on the NPSBN.* *Workgroup members assume "kill" means "prevent access to the network".*	Different
SOR-105.1	The device management network service SHALL allow an authorized entity to install and enable malware/anti-virus protection.	SHALL	SHALL		Same
SOR-106.1	The device management network service SHALL allow an authorized entity to remotely perform a full data wipe of a UE on the network.	SHALL	SHALL		Same
SOR-106.2	The NPSBN SHALL provide for an authorized entity to permanently remove a UE’s ability to access the NPSBN.	SHALL	SHALL	*Redundant to 104.2*	Same
SOR-106.3	The device management network service SHALL allow an authorized entity to temporarily remove a UE’s ability to access the NPSBN.	SHALL	SHALL WITH COMMENTS	*This is a service available to agencies today through enterprise services with cellular carriers, and workgroup members expect no less on the NPSBN.* *Workgroup members assume "kill" means "prevent access to the network".*	Different
SOR-106.4	The NPSBN SHALL provide the ability to lock out NPSBN UEs on commercial carrier networks.	SHALL	SHALL	*SHALL*	Same
SOR-107.1	FirstNet SHALL be responsible for defining a minimum Information Assurance level for PSENs that wish to connect to the NPSBN.	SHALL	SHALL	*SHALL*	Same
SOR-107.2	FirstNet SHALL use appropriate mechanisms to secure and protect user, management, and control plane traffic.	SHALL	SHALL	*SHALL*	Same
SOR-107.3	All links between the PSEN and the NPSBN SHALL be properly protected by FirstNet if they traverse insecure domain/area.	SHALL	SHALL	*SHALL*	Same
SOR-107.4	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.	SHALL	SHALL	*SHALL*	Same
SOR-108.1	If the NPSBN provides a VPN capability, that capability SHALL meet industry acceptable encryption levels for the passing of public-safety grade information.	SHALL	SHALL	*SHALL*	Same
SOR-108.2	The NPSBN VPN capability, if provided, SHALL support VPN clients that are compatible with deployed and supported operating systems.	SHALL	SHALL	*SHALL*	Same
SOR-108.3	User agencies SHALL be permitted to provide their own VPN solutions for accessing their PSEN.	SHALL	SHALL	*SHALL*	Same
SOR-108.4	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.	SHALL	SHALL WITH COMMENTS	*The responsibility to ensure all sensitive traffic is encrypted end-to-end rests on the operating agency.*	Different
SOR-108.5	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,	SHALL	SHALL WITH COMMENTS	*Workgroup assumes that the non-FirstNet UE in this requirement is accessing an*	Different

	or federal statute or policy SHALL be encrypted.			*NPSBN service or application over a commercial network. Otherwise, this requirement would not apply.*	
SOR-109.1	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.	SHALL	SHALL		Same
SOR-109.2	The NPSBN SHALL implement access controls/firewalls to prohibit unallowed network connections and traffic.	SHALL	SHALL		Same
SOR-109.3	The NPSBN SHALL establish procedures for application owners to open required ports and protocols for access control/firewall traversal.	SHALL	SHALL		Same
SOR-109.4	The NPSBN SHALL inspect all network traffic at security boundaries for intrusions.	SHALL	SHALL		Same
SOR-109.5	The NPSBN SHALL inspect all network traffic as possible based upon encryption level at security boundaries for malware and viruses.	SHALL	SHALL		Same
SOR-109.6	The NPSBN SHOULD actively prevent intrusions.	SHOULD	SHALL WITH COMMENTS	*Workgroup members feel that without active intrusion detection, the network can be compromised at a base level.*	Different
SOR-110.1	The NPSBN SHALL monitor and log the transport network for security vulnerabilities and violations with the intent of providing improved application, service, and general availability.	SHALL	SHALL WITH COMMENTS	*Logs SHALL meet legal requirements for state records retention and audits.*	Different
SOR-110.12	Backhaul equipment SHALL be compliant with applicable standards and regulatory mandates.	SHALL	SHALL		Same
SOR-110.2	The NPSBN SHALL maintain a status of network security accessible by PSEN security personnel.	SHALL	SHALL		Same
SOR-111.1	Physical security of sites SHALL prevent unauthorized access.	SHALL	SHALL		Same
SOR-111.2	Local PSEN O&M administrators SHALL be provided with means to monitor alarms in their respective service area.	SHALL	SHALL		Same
SOR-111.3	Outdoor radio sites SHALL be equipped with physical and/or electronic means to detect, monitor, and deter unauthorized entry.	SHALL	SHALL		Same
SOR-112.1	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.'	SHALL	SHALL		Same
SOR-112.2	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.	SHALL	SHALL		Same
SOR-113.1	NPSBN backhaul, transport, and IP packet prioritization techniques SHALL be consistently applied to the entire NPSBN.	SHALL	SHALL		Same
SOR-114.1	On a per-application flow basis, it SHALL be possible for the NPSBN to assign and control the packet latency and packet loss characteristics.	SHALL	SHALL		Same
SOR-114.2	The NPSBN SHALL be capable of determining which application flow a packet is associated with when neither MVPN nor VPN technology is being used.	SHALL	SHALL		Same
SOR-114.3	The NPSBN SHALL be capable of determining which application flow a packet is associated with when MVPN or VPN technology is being used.	SHALL	SHALL		Same
SOR-114.4	It shall be possible for an authorized NPSBN administrator to define templates (groupings) for combinations of packet loss and packet latency rates.	SHALL	SHALL		Same
SOR-115.1	The NPSBN SHALL distinguish between devices from public safety and secondary users during congestion to	SHALL	SHALL		Same

	allow priority access for first responders if needed.				
SOR-115.2	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.	SHALL	SHALL AS AMENDED	*There is no way that a device can be restricted from attempting to access to the network.* *Change to:* *The NPSBN SHALL implement mechanisms to manually restrict secondary user devices from* ***accessing network services*** *at the scene of an incident to minimize system performance degradation.* *This SHALL not affect 9-1-1 calls originated by secondary users.*	Different
SOR-115.3	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.	SHALL	SHALL		Same
SOR-115.4	The NPSBN SHALL provide the ability to manually control access to the NPSBN for different classes of first responders.	SHALL	SHALL NOT	*Read to interpret: "Access" means "ability to access BC14 network" and NOT "ability to configure priority and/or QoS".* *Case: Naval yard shooting; US marshals do not have a role in that incident, so there may be value in moving US marshals to roaming partner so that responding or involved agencies at the incident site have full access to the spectrum on involved sectors* *Lesson learned: With ARMER system, some agencies have busied out channels when responding to incidents. This creates conflict with other agencies that have a right to access that channel.* *New req: The NPSBN SHALL NOT provide the ability to manually control access to BC14 for specific classes of first responders or specific agencies. The intent is to ensure that no individual party has the ability to force any other party off the network on an agency or discipline level. This requirement is not meant to supersede other requirements regarding dynamic priority control.*	Different
SOR-116.1	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.	SHALL	SHALL	*Note amendments to 116.2*	Same

SOR-116.2	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	SHALL	SHALL AS AMENDED	*MN defaults:* *0 (override). Emergency Calls* *1. Mission-Critical Voice (when it is available)* *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* *Minnesota does not anticipate a substantial number of PSEs using the NPSBN for mission critical voice, or for primary voice communications within the launch window of the service or the foreseeable future.*	Different
SOR-117.1	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.	SHALL	SHALL		Same
SOR-117.2	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.	SHALL NOT	SHALL NOT		Same
SOR-117.3	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.	SHALL	SHALL		Same
SOR-117.4	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.	SHALL	SHALL		Same
SOR-117.5	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.	SHALL	SHALL		Same
SOR-117.6	The NPSBN SHALL provide near-real-time usage alerts	SHALL	SHALL		Same

	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.				
SOR-117.7	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.	SHOULD	SHOULD		Same
SOR-117.8	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.	SHOULD	SHOULD		Same
SOR-117.9	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.	SHALL	SHALL		Same
SOR-118.1	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.	SHALL	SHALL		Same
SOR-118.2	It SHALL be possible for an authorized NPSBN administrator (NPSBN and PSEN) to configure which applications can utilize resources previously assigned to other applications.	SHALL	SHALL		Same
SOR-118.3	The NPSBN SHALL support the ability to change whether or not a given application can be preempted, based on triggers from an application or NPSBN-U.	SHALL	SHALL		Same
SOR-119.1	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.	SHALL	SHALL		Same
SOR-119.2	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.	SHALL	SHALL		Same
SOR-119.3	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.	SHALL	SHALL		Same
SOR-119.4	Should pre-emption be required, the NPSBN SHALL first pre-empt secondary user resources before pre-empting any resources used by a primary user.	SHALL	SHALL		Same
SOR-120.1	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.	SHALL	SHALL		Same
SOR-120.2	The NPSBN SHOULD provide an O&M tool to provide the QoS management capabilities described herein (see also Section 6.1.5).	SHOULD	SHOULD		Same
SOR-121.1	The QoS configuration capability SHALL allow suitably authorized public safety O&M users to define/assign QoS roles for their PSE.	SHALL	SHALL		Same
SOR-122.1	Suitably authorized PSE administrators SHALL be able to view a QoS configuration history for users under	SHALL	SHALL		Same

	their authority.				
SOR-122.2	Suitably authorized PSE customer service representatives SHALL be able to view a QoS configuration history for users under their authority.	SHALL	SHALL		Same
SOR-123.1	PSE network managers SHALL be able to view the real-time dynamic priority condition of all users under their authority.	SHALL	SHALL		Same
SOR-123.2	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.	SHALL	SHALL		Same
SOR-124.1	PSE network managers SHALL be able to modify the QoS role of users within their scope.	SHALL	SHALL		Same

APPENDIX 1: WORKGROUP ROSTER

WG Volunteers	Apps / NG911	Devices	Coverage	System / Security
Abley, Brandon[40]	X	X	X	X
Angie Dickison			X	
Beryl Wernberg	X		X	
Brad Peters				X
Bradley Houglum	X	X	X	
Brandon Hendrickson	X			
Brian Askin		X		
Brian Zastoupil			X	
Bruce Hegrenes		X	X	
Chris Kummer	X	X		
Chris Stauffer				X
Corey Zack		X		
Dan Anderson		X		
David J Nault	X			
Diane Wells			X	
Donna Martin				X
Donna Roemmich	X			
Heather Bonnema		X		
Jackie Mines[41]	X	X	X	X
Jake Thompson				X
Jayme Carlson		X		
Jeremy Cossette	X	X	X	
Joel Robak			X	
John Tonding[42]	X	X	X	
Jon Eckel	X	X		
Kate Anich		X		
Kathy Nelson, PE			X	
Kathy Struffert			X	
Kevin Haney		X	X	X
Kristen Lahr	X	X		
Laura Anderson				X
Marcus Bruning[43]	X	X	X	

[40] Project staff, Televate and workgroup facilitator.

[41] Project staff, state of Minnesota.

[42] Project staff, state of Minnesota.

[43] Project staff, state of Minnesota.

WG Volunteers	Apps / NG911	Devices	Coverage	System / Security
Mark Navolio[44]	X	X	X	
Marti Higgs	X			
Mary Borst				X
Mike Martin				X
Nancy Schafer	X			
Peter Gamache				X
Randy Donahue	X	X	X	X
Rick Burke[45]	X	X	X	X
Rick Juth[46]	X	X	X	X
Rodney A. Olson		X	X	X
Rowen Watkins				X
Scott Busche				X
Scott Reiten	X			
David Deal		X		X
Stefanie Horvath				X
Tina McPherson	X			
Tom Vanderwal	X			
Travis Marttila				X
Vince Regan	X			

[44] Project staff, Televate.

[45] Project staff, Televate.

[46] Project staff, state of Minnesota.

APPENDIX 2: WORKGROUP CHARTERS

MNFCP WORKING GROUP CHARTER – Applications and NG911

Vision/Mission:

With the advent of a common National Public Safety Broadband Network (NPSBN) the level of interoperability will be determined by data and applications standards. The Applications Subcommittee is responsible for identifying applications and their requirements for the NPSBN. While the NPSBN can and should support all broadband applications found on commercial wireless networks, a distinction between those generally used and those uniquely required by public safety must be made. The applications subcommittee will be tasked with the following:

Action Items/Goals

- Assess the typical applications required by the public safety personnel; examples:
    - Records Management System, Incident Command support, Prioritization/traffic management/data flow/QOS, Logging/storage/records/legal discovery support, Video & Photographs, Telemetry, Biometrics, Fingerprints, Vital Sign/Biometric Monitoring, Radio-over-LTE, VoLTE,
    - Identify Minnesota specific applications
    - Review potential future applications
- Review CAD-RMS incident data and identify incident types
- Assess each incident type and identify the type of application that would be used during the incident
    - Correlate all incidents with applications
    - Assess the priority of incident
    - Assess the application performance requirements
    - Identify unique requirements such as assigning
        - the priority of uses and secondary users
    - Assess general usage cases and likely devices per incident type
- Develop a list of NPSBN public safety applications
    - Assess whether the application is mission critical to supporting the incident

Deliverables:

1. Initial list of NPSBN PS applications
2. Table Incidents vs. Applications vs. Priority
3. User Group Survey Question Recommendations
4. Application Recommendations

MnFCP Working Group Charter – Devices

Vision/Mission:

The Subcommittee will assess the device requirements, including functionalities, quantities and timeline, to be used by subscribers on the National Public Safety Broadband Network (NPSBN) for the state of Minnesota. Requirements will be assessed for each public safety agency or other organizational type with subscribers on the NPSBN that defines a user group. A sampling of more specific requirements includes:

Action Items/Goals

- Review cost versus device functionality
- Review & comment on various resources
    - NPSTC SOR (earlier versions)
    - FirstNet RFI for devices
- Review preferred device type by incident type and user group
    - What do they do with their personal devices at the incident?
    - Expected Cost; assess tolerance of different price points
- Primary Purpose: Develop an inventory of all devices types complete with a summary features and functionality:
    - Device Types; and what are the specific requirements for each:
        - Smartphone
        - Tablet with embedded modem
        - Computer with embedded modem
        - Vehicular Modem, & Router (trunk mounted with Ethernet connection)
        - USB Modem
        - Other?
    - Form Factor Characteristics
        - Hardening, Buttons, (e. g., PTT , emergency), Qwerty Keyboard, Glove-friendly, Screen size
    - Functionality
        - Bluetooth, Wi-Fi, WLAN, Commercial Carrier Roaming
        - Dual mode LMR/P25
        - Supported Operating System (OS)
        - Geolocation (GPS, GLONAS, dead reckoning, altimeter, and others)
        - Tethering, Serial Port, Near-field communications
    - Review of Risks and assess the Tolerance by the State: Will the public safety device keep pace with the commercial technology in the marketplace?
- Assess BYOD device requirements for those agencies that will be purchase their own device
    - Open vs. Close Garden approach for BYOD devices
        - Dual personality (separate workspace/profile/functionality)
- Priority of device Types; which ones would they like to have on the market first?

Deliverables:

1. Identify preferred Form Factor and Functionality Requirements per Device Type; any specific requirements per device
   a. Requirements for BYOD devices
2. Final Device Recommendation

MnFCP Working Group Charter – Service Area

Vision/Mission:

The Service Area workgroup will determine the basis for evaluating the National Public Safety Broadband Network (NPSBN) coverage or service areas within the State. In addressing coverage this workgroup will need to include the outputs of the applications and devices workgroups; because the both affect the availability of coverage, the sufficiency of throughput and the usage requirements. The workgroup will assess the requirements for mobile / portable, indoor / outdoor coverage for each application category (voice, video) and each user group. Coverage augmentation strategies and other temporary coverage enhancement options, for use in primarily rural areas, will be reviewed, assessed and evaluated. The process includes:

Action Items/Goals

- Review key NPSBN user groups
- Review key device categories
- Review application categories and their usage scenarios
- Review Coverage Augmentation Strategies:
  - In-vehicle and other based portable relays, femtocells, gateways, COWS
- Determine bandwidth requirements
- Determine Indoor/Outdoor coverage types
- Determine Mobile/portable coverage types

Deliverables:

1. Draft Coverage Categories
2. **2.** Draft preferred strategies and requirements for Coverage Augmentation

MNFCP WORKING GROUP CHARTER – SYSTEM AND SECURITY

Purpose:

The Minnesota and FirstNet Consultation Project (MnFCP) workgroups will define Minnesota's requirements for System and Security for incorporation into the Minnesota and FirstNet consultation process. These requirements will be developed by Minnesota stakeholders and thought-leaders and endorsed by the SECB to ensure that they accurately reflect user requirements. This is one of four workgroups that have been commissioned to define Minnesota user requirements for FirstNet.

Goal:

Identify the security and system architecture and performance requirements for the PSBN. A key and important output of this workgroup will be the contents of a Service Level Agreement (SLA) for the State of MN for PSBN service. This SLA will form the basis of the State's tangible requirements for overall service before FirstNet and will build upon any SLA requirements initiated by other workgroups. Estimated effort: 24 hours each participant over a period of three months.

Deliverable:

Upon completing the working sessions, Televate will produce a written report with a distinct section reflecting the findings of each MnFCP workgroup. The report will document the workgroup's requirements and describe the methodology for collecting them. The final meeting of each workgroup will be devoted to reviewing the draft report section for the group and resolving any issues or comments.

- Overview
- MnFCP Service Area Requirements
- MnFCP Devices Requirements
- MnFCP Applications Requirements
- MnFCP System and Security Requirements
- Methodology
- Areas for Future Study

Methodology

Working Meetings

Meetings will be held via Webex and conference call on a weekly basis. Two weeks prior to the first meeting, Televate will send out a poll via Doodle to establish a regular meeting time. This meeting time will be the regular meeting time for the group for the remaining meetings. Meetings will begin in January 2015 and will conclude March 2015.

Asynchronous Collaboration

Televate will provide the group with materials to review in-between meetings, including draft requirements, NPSTC excerpts and survey tools to collect the group consensus. Participation in these asynchronous collaboration sessions is required of the group to ensure that the group is productive and successful.

Ideal Membership:

- Technical staff (e.g., radio)
- IT staff
- Information Security Experts

Workgroup Action Items:

- Review group scope, purpose and action items
- Document Minnesota information security requirements for public safety
- Develop SLA contents for PSBN service
- Review NPSTC requirements related to system and security
- Review architectural requirements for the NPSBN in Minnesota
- Review Service and interoperability requirements for the NPSBN in Minnesota