



BEFORE THE

FIRST RESPONDER NETWORK AUTHORITY

*First Responder Network
Authority (FirstNet)
Nationwide Public Safety
Broadband Network (NPSBN)
Special Notice*

Solicitation Number: D15PS00295B

COMMENTS OF THE STATE OF OHIO

Introduction

The state of Ohio, through the OhioFirst.Net program and its Statewide Interoperability Executive Committee is pleased to have the opportunity to comment on FirstNet's Special Notice and Draft RFP for the Nationwide Public Safety Broadband Network. We congratulate FirstNet on taking extraordinary efforts in recent months to provide transparency into and to seek stakeholder feedback on its strategic planning and procurement strategy.

That said, there are a number of issues in the Special Notice that are of concern to our stakeholder community.

First, and foremost, we strongly urge FirstNet to consider existing commercial coverage as a primary metric in reviewing vendor proposals. Regardless of whether FirstNet positions itself as a competitor to commercial cellular carriers or not, the organization must acknowledge that first responders are using commercial wireless service today, are very satisfied with their service, and will compare FirstNet's offering to it.

We also request that FirstNet includes state agency-developed data in its final procurement. Ohio is performing deep-dive coverage reviews with every county and major market in the State. These reviews will provide FirstNet with coverage needs that stakeholders feel a great deal of ownership in and will ensure a much higher degree of success than FirstNet's baseline, which is based purely on data and which was developed without individual stakeholder interaction.

Additionally, we are very concerned that FirstNet did not include an SLA in its draft RFP. FirstNet's featureset and buildout timeline are relatively meaningless without being accompanied by an SLA, and it is difficult for stakeholders to comment on the merit of the service without having any insights into the level of service users can actually expect. We have included in our response some sample data and reference documents to provide FirstNet background on what users in Ohio will expect when FirstNet does ultimately publish an SLA.

Finally, the definition for rural coverage milestones that FirstNet has introduced is completely inadequate and is contradictory to FirstNet's baseline coverage model. Below, we provide our



interpretation of FirstNet’s definition, how it would apply to our state, and why we feel that FirstNet is providing conflicting information about what its actual intended rural commitment is.

This document was reviewed and approved by the Nationwide Public Safety Broadband Network Subcommittee of the Ohio Statewide Interoperability Executive Committee and carries the committee’s full endorsement.

Comments on Coverage Model (Appendix C-1)

FirstNet’s baseline coverage model does not depict stakeholder needs in a meaningful way that stakeholders can take ownership of and present to their constituencies to make a justification to adopt the service. Acknowledging that FirstNet presents this baseline model as “a starting point to identify potential public safety priority for permanent terrestrial coverage”¹, and therefore we assume FirstNet anticipates the final coverage requirement to be substantially different, we propose two substantial factors from which we strongly recommend FirstNet bases its final coverage requirements for Ohio: (1) Commercial carrier coverage and (2) County-by-county coverage reviews.

Commercial Carrier Coverage

We strongly urge FirstNet to consider existing commercial carrier coverage as a primary metric in evaluating vendor proposals.

We acknowledge that FirstNet was not created to compete directly with commercial carriers; the purpose of FirstNet is to provide a mission-critical public safety broadband network and **is not** to establish a government-backed commercial cellular carrier to take business from the private market. However, FirstNet is offering a service that public safety organizations will have to be compelled to adopt in favor of service with a commercial cellular carrier; in effect, FirstNet’s de facto competition is the incumbent commercial cellular market.

However, the baseline coverage model does not consider existing commercial carrier coverage at all. We acknowledge that commercial carriers are continuously upgrading their networks, and so matching their service presents a moving target. But whatever metrics FirstNet includes in its procurement, it cannot and will not be able to avoid comparisons to the incumbent option—existing commercial carriers, with whom most public safety agencies are presently very satisfied.

¹ See Special Notice D15PS00295 (“Notice”), Appendix C-1 at 1

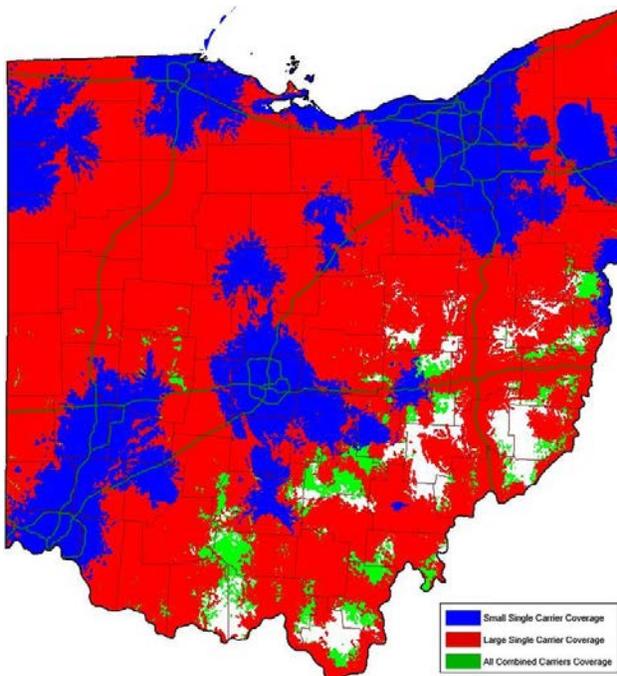


Figure 1: Existing Cellular Carrier Coverage in Ohio

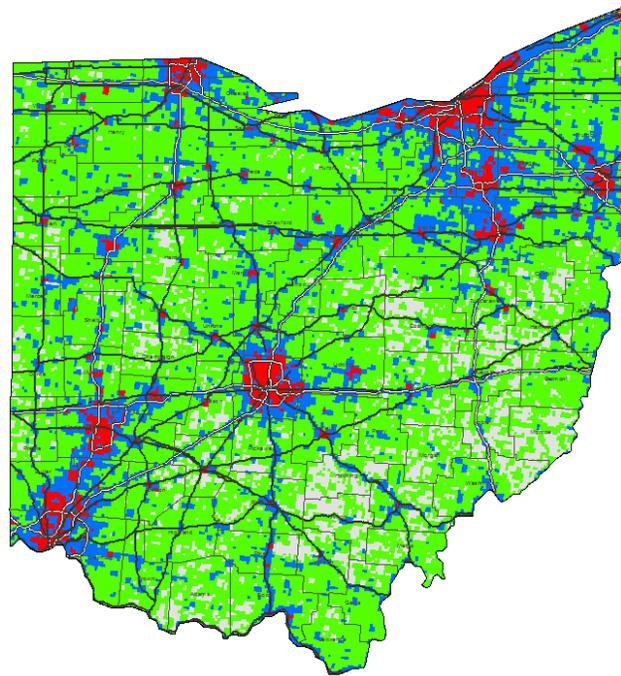


Figure 2: FirstNet Baseline Coverage for Ohio

Figure 1 shows existing aggregate cellular carrier coverage in Ohio based on publicly-available information. While existing coverage compares closely with FirstNet’s baseline model, it does not appear from the Special Notice that existing coverage was considered in the baseline coverage model. We feel that this is a tremendous oversight. FirstNet must directly address the immediate, obvious and viable alternative to FirstNet’s service offering. FirstNet must offer something that public safety agencies can justify switch to from a service that public safety users are already very satisfied with.

County-by-County Coverage Reviews

FirstNet’s model is based exclusively on data, including a distribution of public safety users, high-risk areas, US population, developed areas and roadways.² While this data is certainly relevant and useful for building a baseline need, it is not based on actual user requirements and does not target a need expressed by the target customer base. We propose that FirstNet bases coverage requirements in its procurement for the state of Ohio on our targeted, county-by-county coverage and needs assessments.

Through the Ohio-FirstNet Implementation Project (OFIP), we are performing detailed, county-by-county coverage and needs assessments with each county, each major city, each major state agency and a small number of special entities (e.g., a public utility or mining company) to determine each agency’s needs. These coverage reviews provide each stakeholder with the opportunity to review FirstNet’s coverage baseline, articulate their needs, ask questions about the program and, most importantly, take ownership over their own requirements.

² See Notice, Appendix C-1 at 2



The primary output of these coverage reviews will be a set of GIS polygons depicting priority coverage areas. ATST will work with the OFIP Workgroup and the state to determine how to label these areas; for example, to fit into FirstNet deployment phases.

Each coverage review includes both objective and subjective inputs—we will reference FirstNet’s baseline coverage model, historical CAD data and other factors including commercial carrier coverage—as well as subjective inputs gathered during interviews. We will then aggregate all inputs and define priority coverage zones according to FirstNet phased buildout requirements. The ultimate output is easy-to-interpret, visual coverage objectives that stakeholders can claim ownership of and use to justify their argument to migrate to FirstNet in front of their own constituencies.

We will begin these reviews in August 2015, and they will take approximately one year to complete; we readily acknowledge that FirstNet’s data collection deadline will have well passed by the time we complete our work. However, we will deliver our final coverage review data to the state well before FirstNet negotiates a final RFP or delivers a state plan. We urge FirstNet to structure its vendor RFP in such a way that vendors can consider our county-by-county coverage reviews in preparing their response.

Comments on SLA Requirements (Appendix C-2) and Minimum Recommended Technical Requirements (Appendix C-3)

FirstNet did not include SLA requirements in its special notice, as these requirements “. . . are still being developed in consultation with states, tribes, territories, public safety stakeholders, and market participants, and may be provided at a later date or in a subsequent RFP.”³ While the Notice certainly includes a number of measurable and specific factors to evaluate, we feel that it is very difficult to comment on the Notice as a whole without seeing the proposed terms of FirstNet’s SLA. The level of commitment of service—availability, response windows, support, remuneration of damages, dispute resolution, exceptions and many other factors—will drive the cost for vendor proposals and, in turn, FirstNet’s cost.

We offer, for reference, the Ohio-MARCSIP Service Terms and Conditions and a draft sample of Ohio’s Launch Requirements for FirstNet.

Ohio-MARCSIP Service Terms and Conditions

MARCSIP (Multi-Agency Radio Communication System-IP) is a 700/800 MHz Project-25 radio and data network that provides service to its subscribers throughout Ohio and within an approximate 10 mile radius outside of Ohio. The MARCS system provides statewide, secure, reliable public service wireless communication for public safety and first responders.

³ See Special Notice: *FirstNet’s Nationwide Public Safety Broadband Network (NPSBN)*, Solicitation Number: D15PS00295B; retrieved 7/21/2015 at https://www.fbo.gov/?s=opportunity&mode=form&id=55fa4d3227d5ac0173e4613e04368c86&tab=core&_cview=1.



MARCSIP is required to provide a minimum of 97.5% mobile voice and data in street coverage throughout the state; in reality, the system provides 99.71% aggregate voice and 98.13% aggregate data coverage and is used by over 54,000 first responders throughout the state of Ohio.

The MARCSIP Service Terms and Conditions document represents the system SLA; it specifies who is eligible as a public safety user, commitments and responsibilities for MARCSIP users, MARCS, and penalties for failing to fulfill one's responsibilities under the agreement.

The Terms and Conditions for MARCSIP are by no means a comprehensive model for FirstNet's SLA for broadband communications. However, we present this document to communicate user expectations; public safety agencies throughout the state of Ohio will expect a level of service comparable to or greater than MARCSIP: nearly 100% land area coverage throughout the state and service availability nearly 100% of the time. Whether these terms are reasonable or not—FirstNet will be unable to avoid a comparison to MARCSIP's excellent service provided to our users.

Draft Statement of Requirements for FirstNet Launch

Ohio's Statement of Requirements for FirstNet is Launch based closely off of NPSTC's similarly named document: NPSTC's Public Safety Broadband High-Level Launch Requirements for FirstNet Consideration.⁴ In developing these requirements, we put together three subject-matter specific workgroups to carefully review *every* NPSTC launch requirement, discuss its applicability and merit to Ohio, and to provide modifications or commentary as necessary.

This set of requirements effectively represents Ohio's SLA requirement for FirstNet. FirstNet's State Plan (or an alternative, opt-out vendor's plan) will be evaluated against these requirements. **In developing its SLA terms, we strongly advise that FirstNet (1) consider the NPSTC SOR as a baseline in developing its SLA commitments and (2) consider, when procuring for Ohio, our unique modification to the NPSTC SOR.**

We acknowledge that FirstNet has introduced the 2012 *FCC Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*⁵ as a set of minimum technical requirements for the network. Our workgroup based its work off of NPSTC's requirements because we felt the FCC requirements were not specific or substantial enough. We also understood that NPSTC's launch requirements were developed with substantial public and private input and that they accurately reflect the needs of the stakeholder community.

⁴ Retrieved 7/21/2015 at

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

⁵ Retrieved 7/21/2015 at

https://www.fbo.gov/?s=opportunity&mode=form&id=55fa4d3227d5ac0173e4613e04368c86&tab=core&_cview=1.



Comments on Definition of Rural Coverage Milestones (Appendix C-8)

FirstNet's proposed rural coverage milestones appear to describe very little of the geography of Ohio. **We request that FirstNet clarifies its definition of "rural" to better meet its objectives to provide substantial service to rural areas throughout the State.**

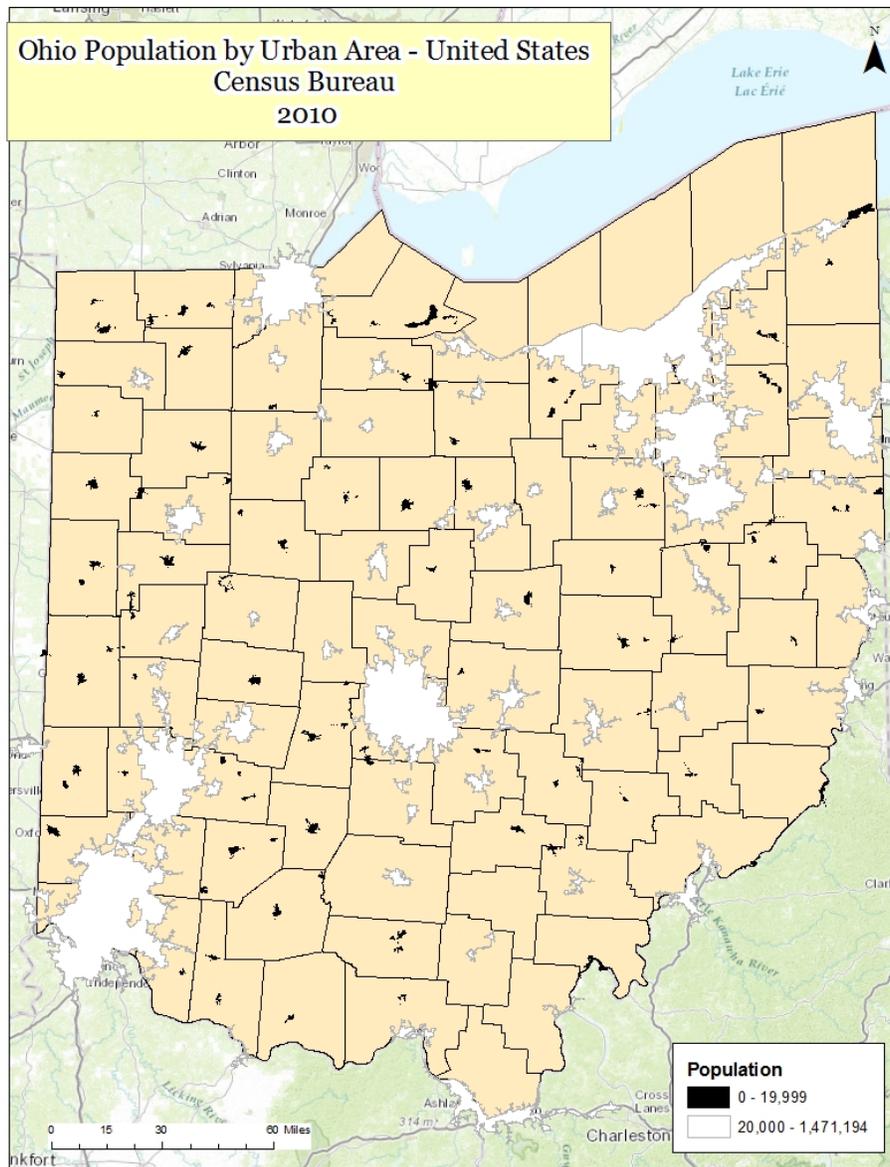


Figure 3: Jurisdictional Areas of Cities and Towns with over 20,000 Residents in Ohio



Per the Act, FirstNet is held to “Substantial rural coverage milestones”.⁶ In this Notice, FirstNet introduces a new definition of “rural”: “. . . a city, town or incorporated area that has a population of less than 20,000 inhabitants.”⁷ Figure 3 below illustrates all jurisdictions in Ohio that would fit FirstNet’s definition of “non-rural”. Using jurisdictional boundaries as a reference, as indicated in the figure, 4,987 sq. mi. or 12% of the land area of the state would be considered “non-rural” by this definition and 36,700 sq. mi. or 88% of the state would be considered “rural”.

FirstNet proposes that its “Substantial Rural Milestones” will be fulfilled if “[a]t least 20 percent (20%) of total covered area for each Band 14 IOC deployment [. . .] comprise[s] areas defined as rural (coverage measured in square miles)”, starting after year 1 of construction (IOC 2-5).⁸

Table 1: Land Area of Ohio and FirstNet Proposal Total Category and Milestone Land Areas

State of Ohio Land Area, sq. mi.	Non-Rural/ Pops 20,000+, sq. mi.	Total Rural, sq. mi.	Rural Milestone Area , sq. mi.
41,687	4,987	36,700	997

Using the jurisdictional areas of cities and towns in Ohio and FirstNet’s proposed rural milestones, this means that **FirstNet’s total rural coverage commitment is only 997 sq. mi. or only 2% of the State.** By no means is it likely that FirstNet in fact intends to cover *only* 14% of the entire state (12% non-urban areas and 2% rural buildout milestone). Not only is it unacceptable to users that FirstNet would provide terrestrial coverage to only 14% of the state, the milestone is also inconsistent with FirstNet’s baseline coverage model (see [Figure 2](#) above) which shows terrestrial coverage in the *majority* of the state.

We acknowledge that FirstNet’s minimum rural coverage milestone target will likely represent less land area than the final realized coverage—meaning, FirstNet will provide more coverage than its minimum target. However, a literal reading of FirstNet’s proposed milestone sets its total rural buildout obligation to 997 sq. mi. of the state. We feel it is not reasonable that FirstNet should set such a low bar for itself.

Therefore, we request clarification and request that FirstNet considers adopting a different definition for its “rural buildout milestone” that reflects a more robust level of coverage, more accurately represents our stakeholder coverage needs and is more consistent with FirstNet’s proposed coverage baseline.

Conclusion

The state of Ohio deeply appreciates the opportunity to provide feedback on FirstNet’s procurement planning.

⁶ See Act at 6206(b)(3).

⁷ See Notice, Appendix C-8 at 4.

⁸ See Id.



As described above, we feel that FirstNet has not considered the proper factors in developing its coverage baseline and we advise FirstNet to give greater consideration to incumbent commercial wireless providers as well as agency-developed coverage requirements. We are very concerned that FirstNet has not published an SLA and have provided information to equip FirstNet with some knowledge of the level of service users in Ohio will expect. Finally, we request that FirstNet provides clarification on its definition of rural coverage milestones, makes a greater commitment to rural areas and brings its rural coverage milestones in line with coverage requirements developed by FirstNet as well as user agencies.



Appendix I: OFIP Coverage Review Labor Description



ADD TASK 13: COUNTY-BY-COUNTY REVIEWS

FirstNet’s data collection category task 2: Operational Areas requests under category (2) Users and their Operational Areas. The following task, **Task 13: County-by-County Reviews**, is designed to meet sections (2c-i) *user maps based on jurisdiction* and (2c-ii) *common response areas* through performing individualized county-by-county reviews.

SUMMARY

We propose conducting an individual coverage and needs review with each county, each major city, each major state agency and a small number of special identities (e.g., a public utility or mining company) to determine coverage needs. These coverage reviews provide each stakeholder with the opportunity to review FirstNet’s coverage baseline, articulate their needs, ask questions about the program and, most importantly, take ownership over their own requirements. Approximately 1/3 of coverage reviews will be completed with an on-site resourced; the rest will be handled exclusively via WebEx.

Each coverage review includes the following tasks:

- Email contact and read-aheads
- CAD data processing
- Coverage Review
- Follow-up and Verification

EMAIL CONTACT AND READ-AHEADS

ATST will first make email contact with the individual identified in our POC survey to schedule the meeting. We will send read-aheads including:

- OFIP publications 1 and 3
 - Program Overview (#1)
 - Special coverage review publication (#3)
- Training modules 1, 2 and 3
 - What is broadband?
 - What is LTE for FirstNet?
 - Consultation Objectives

ATST will utilize email marketing software and site analytics to provide detail on stakeholder engagement with read-aheads.



CAD DATA PROCESSING

ATST will make a CAD data request of incident data dating back three years. We will use this information to produce a heatmap that will be overlaid on top of FirstNet’s baseline coverage objectives. An early prototype basemap from a project in Minnesota is depicted below.



Figure 1: Sample Heatmap

The heatmap depicts density of incidents throughout the stakeholder’s service area. Our research has found that while incidents *tend* to cluster around populated areas and that incident data *tends* to correspond by population, these trends are not universal. For example, recreational areas will be excluded from a map that heavily leverages population density even though they are high-risk response areas. This underlying data provides a scientific basis for making a claim for a coverage need before FirstNet.

Furthermore, the CAD data provides ancillary benefit to the public safety agency. Our research shows that, generally, this kind of analysis has not been done by most public safety agencies throughout the country. Our data models can be leveraged by the agency to justify future public safety programs independent of FirstNet and can additionally provide a framework to define data applications of interest for supporting incident response, and can be further leveraged to conduct network capacity planning based on user projected application requirements per incident type. The CAD data provides an extensive baseline of valuable information to facilitate, coverage, application and capacity analysis and planning.

Constraints

We cannot expect 100% of agencies to provide usable CAD data throughout the state. For example, some agencies do not geocode incidents in a usable format, might use a proprietary data format, might not be able to produce a data report or in some rare cases do not utilize CAD at all.

ATST will provide the agency with a baseline data format and make a best-effort attempt to convert their data to a common format. If the agency cannot comply, ATST will not utilize its CAD data and will report the exception to the state.



COVERAGE REVIEW

ATST will perform a coverage review via WebEx and, in about 1/3 of markets, compliment the WebEx survey with a face-to-face resource. The coverage review will include:

- An introduction to the project
- A review of FirstNet baseline coverage data
- A review of commercial carrier services in their area (marketed vs. actual end-user experience)
- A review of incident data
- Program Q&A

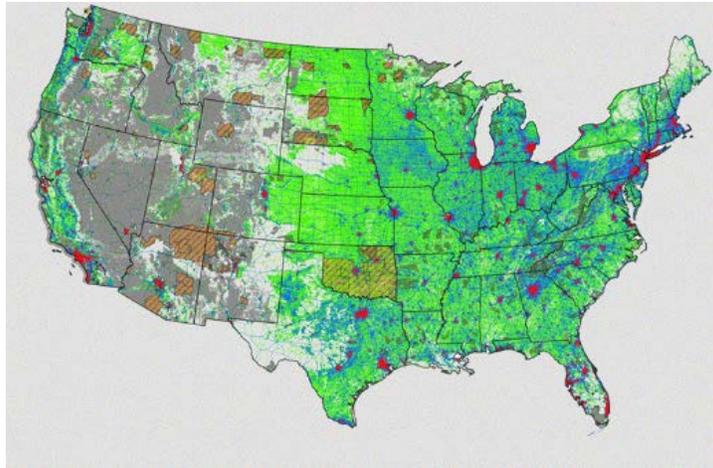


Figure 2: FirstNet Baseline Coverage Model

The primary output of these coverage reviews is a set of GIS polygons depicting priority coverage areas. ATST will work with the OFIP Workgroup and the state to determine how to label these areas; for example, to fit into FirstNet deployment phases.

List of Coverage Reviews

- 88 counties
- 10 “top 10” markets (as determined by the state; includes populous cities, counties or other special markets)
- 5 state agencies
- 5 special entities (potential private sector user entities, additional state agencies, additional top 10 markets, additional “redo” reviews or any other entity at the state’s direction)



Constraints

Our prior experience indicates that approximately 2-4% of coverage reviews will be unsuccessful, primarily due to the unavailability of key participants who may be called away to emergency response or other unexpected conflicts, and will have to be repeated. We have included in our estimate a margin of error to accommodate **up to 5 “redo” coverage reviews.**

FOLLOWUP AND VERIFICATION

ATST will perform follow-up with the agency to verify results of the coverage review, including reviewing coverage priority polygons and evaluating customer satisfaction. Finally, we will utilize these follow-up interviews to encourage contacts to review the POC survey.

TRAVEL

This task includes travel. These trips will **NOT** come out of the project general travel pool and are included in the task cost.

- 20 Remote Staff Trips
- 48 Local Staff Trips

DELIVERABLES

- Meeting Content and Review Process Document
- Review with 22 of 88 Counties
 - CAD Data
 - Heatmaps
 - Coverage Objectives Polygons
 - Notes and Lessons Learned
- Review with 44 of 88 Counties
- Review with 66 of 88 Counties
- Review with 88 of 88 Counties
- Review with 5 of 10 Top 10 Markets
- Review with 10 of 10 Top 10 Markets
- Review with 5 State Agencies
- Review with 5 Special Entities
- Final Report



Appendix 2: Ohio-MARCSIP Service Terms and Conditions



MARCSIP SERVICE TERMS AND CONDITIONS

SECTION 1: DEFINITION OF CONTRACTUAL PARTIES

1.1 MARCS (Multi-Agency Radio Communication System) is a 700/800 MHz radio and data network that utilizes state-of-the-art trunked technology to provide statewide interoperability in digital clarity. MARCSIP provides statewide radio coverage for police, fire and EMS services, and other public agencies that serve as first responders or contribute materially to homeland security.

1.2 A MARCSIP Service Subscriber is a public or private entity which provides first responder services to the public and materially contributes to homeland security.

1.3 A MARCSIP Service Subscriber may be an equipment vendor utilizing subscription services for the sole purpose of demonstrating radio service to potential customers.

1.4 A MARCSIP Service Subscriber may be a public or private school district within the state of Ohio.

SECTION 2: SCOPE OF SERVICE

2.1 MARCS agrees to provide subscriber with MARCSIP service based upon subscriber purchasing MARCS compatible radios and equipment.

2.2 MARCS provides statewide interoperability in digital clarity to its subscribers throughout Ohio and an approximate ten (10) mile radius outside of Ohio.

SECTION 3: TERMS

3.1 Initial Term: The Service Subscription Agreement shall commence on the date of the last signature thereto and shall continue until the last day ending the current state fiscal biennium, on June 30th.

3.2 Renewal Term: The Service Subscription Agreement shall automatically renew every two years on July 1, coinciding with the beginning of each new state biennium, and otherwise upon the same terms and conditions as are set forth herein, unless 30 days prior to the end of the biennium, Subscriber provides MARCS with written notification of its intent not to renew.

SECTION 4: MARCS' RESPONSIBILITIES

4.1 MARCS agrees to:



- 4.1.1 Provide continuous system availability from all towers and central equipment infrastructure. Continuous system availability means 24 hours a day, 7 days a week for 365 days a year.
- 4.1.2 Provide continuous access to live help via the network operations center (866-OH-MARCS) to assist subscriber if subscriber is experiencing any technical or operational difficulties.
- 4.1.3 Work with subscriber to develop talk group plans, including but not limited to subscriber specific talk groups based on the subscriber's mission and agents deployed and need for interoperability within their geographic location.
- 4.1.4 Approve additional radio unit activations. Approval of additional radio unit activation shall include but not be limited to the outcome of grade of service (GOS) studies which shall be performed by the MARCS Program Office. The GOS is a way of assuring that the additional devices will not adversely affect current communications on the MARCSIP system.

SECTION 5: SUBSCRIBER'S RESPONSIBILITIES

- 5.1 Subscriber agrees to:
 - 5.1.1 Maintain and repair all units used for the subscription service;
 - 5.1.2 Limit the use of radio to public safety or first responders; and
 - 5.1.3 Not use profanity over the system
- 5.2 Subscriber shall be responsible for the proper use of devices subscribed to MARCS. Subscriber agrees to follow proper FCC and MARCS' radio protocol at all times (e.g., utilization of radio codes to shorten transmissions, transmission breaks during lengthy traffic, deferral to emergency traffic, etc.). At MARCS' sole discretion, improper use of device may result in the suspension or termination of executed agreement without refund of any fees paid.
- 5.3 Subscriber shall not sublet activated devices or assign any subscription services to any individual, agency or organization, without the express written consent of MARCS.
- 5.4 Subscriber shall submit to MARCS their contact information and a list of the serial numbers for all radios utilizing the subscription services on the Device Information Excel form posted to our website at <http://das.ohio.gov/MARCS> under the Subscriber Process.
- 5.5 Subscriber shall notify MARCS if there is any change in their equipment inventory, including but not limited to lost/stolen devices or additional devices activated utilizing the subscription service.
- 5.6 Subscriber shall work with MARCS' voice radio services staff to develop the proper talk groups in order to forward the mission of the subscriber, without negatively impacting the MARCS radio system. Subscriber understands these talk groups will include the MARCS interoperability talk groups, as detailed in MARCS Policy MPP-15.0 posted to our website at <http://das.ohio.gov/MARCS> under the Policies.



5.7 Subscriber shall be responsible for all equipment and installation costs associated with the system infrastructure upgrade if it is determined by MARCS that the addition of channels and/or frequencies is necessary in order to accommodate any additional radio units. MARCS, at its discretion but upon providing prior written notification to Subscriber, shall install at Subscriber's expense any additional equipment that MARCS deems necessary. Subscriber agrees that upon installation of any equipment on the system infrastructure, the equipment becomes the permanent property of MARCS and MARCS shall be responsible for maintenance of the equipment.

SECTION 6: SUBSCRIBER INVENTORY GUIDELINES

6.1 Subscriber's initial inventory shall consist of the original list of devices to be activated for service as submitted to MARCS via the Device Information Excel form posted to our website at <http://das.ohio.gov/MARCS> under the Subscriber Process.

6.2 Subscriber's additional inventory shall consist of any additional devices submitted to MARCS for service activation via the Device Information Excel form posted to our website at <http://das.ohio.gov/MARCS> under the Subscriber Process; or activated devices transferred from another subscriber's inventory to subscriber's inventory via the Equipment Transfer Receipt Form posted to our website at <http://das.ohio.gov/MARCS> under the Subscriber Process.

6.3 In the case of an inventory transfer from one agency to another which results in the transfer of the user fee as well, Subscriber shall continue to be responsible for the user fee of transferred inventory until the next regularly scheduled billing cycle.

6.4 Subscriber's inventory is subject to quarterly and annual audits by MARCS. MARCS reserves the right to change or update Subscriber's inventory at any time. All changes to Subscriber's inventory initiated by MARCS shall be reflected in a letter amendment to the executed agreement acknowledged by both parties.

6.5 If an inventory discrepancy is discovered at any time, all affected parties agree to resolve the discrepancy. Billing will continue based on the corrected inventory. If additional fees are due as a result of the discrepancy, MARCS will invoice Subscriber and Subscriber agrees to pay any additional fee amount in the next quarterly payment. If necessary, MARCS may credit subscriber any service fee credit due up to one quarter in arrears.

SECTION 7: INVOICING AND PAYMENT OF SERVICES

7.1 Invoicing for subscription services will begin upon the activation date of device. "Activation date" is defined as the date upon which the device is programmed and in the control of the subscriber.

7.2 Unless otherwise indicated on the MARCSIP Radio Information form, all devices will be invoiced in advance on a calendar quarterly basis. Subscriber may elect to be billed in advance on an annual basis. Annual



invoices are based on the state fiscal year and are billed and mailed in July covering the July through June service period.

7.3 MARCSIP services will be invoiced at the current, statewide rate in effect at the time of invoicing.

7.4 While MARCS does not anticipate any significant modifications to service fees, Subscriber acknowledges that new assumptions may drive changes in the subscriber fee for the MARCSIP system. MARCS will notify Subscriber of future rate changes for the MARCSIP system ninety (90) days prior to the effective date of change.

7.5 All invoices are due and payable upon receipt. If Subscriber feels a discrepancy has occurred in the amount of the invoice, Subscriber will have ninety (90) days after receipt of invoice to dispute the invoice amount. After that, all undisputed invoices shall be deemed payable as is.

7.6 If the invoice is not paid by the subscriber when due, MARCS holds the right to charge a late fee of 1.5% per month. The invoice paid by subscriber shall be due without set off notice or demand from MARCS.

7.7 Once invoiced, any payment made by subscriber shall contain a notation of the invoice number and shall be made payable to the Treasurer, State of Ohio MARCS 5C2 Fund. Payment should be mailed to:

Treasurer, State of Ohio (Fund 5C2)
Office of Information Technology
c/o Finance Office
30 East Broad Street, 40th Floor
Columbus, Ohio 43215-3414

SECTION 8: MISCELLANEOUS

8.1 Changes or alterations to the original preprinted text and terms of this document shall not be honored.

8.2 This MARCSIP Service Terms and Conditions document supersedes any and all previous service documents.

8.3 This document shall be governed, construed and interpreted in accordance with the laws of the State of Ohio.

8.4 All parties agreeing to these terms and conditions further agree that they are in compliance with the requirements of Ohio Revised Code Section 125.111



Appendix 3: OFIP Draft Launch Requirements

See Separate file: OFIP_Draft_Requirements_for_FirstNet_at_Launch.xlsx

The attached is an excerpt from an OhioFirst.Net Statement of Requirements for Launch document, a forthcoming project deliverable. These requirements are adapted from NPSTC's Public Safety Broadband High-Level Launch Requirements Statement of Requirements for FirstNet Consideration (SOR).

These requirements are in draft form and are provided for reference and context for this filing only; the OFIP Statement of Launch Requirements will supersede this document upon its publication.

This table includes the following fields:

Source

The source of the requirement number. Requirements copied from the SOR are marked "SOR", while those unique to Ohio's workgroup are marked "OH".

Description

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

OH

Ohio'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 "OH" fields match.

Source	Description	SOR	OH	Comments	Comparison
OH	Priority of Public Safety Traffic SHALL be maintained throughout the entire NSBN, including on the backhaul network.	N/A	SHALL		N/A
OH	All VPN solutions deployed on the NPSBN shall meet industry acceptable encryption levels for the passing of public-safety grade information.	N/A	SHALL		N/A
OH	FN SHALL provide neutral transport of PSEN traffic when required by the PSEN.	N/A	SHALL		N/A
OH	Devices SHALL support dual-SIM configuration so that PSEs can co-exist on multiple networks, with multiple service accounts, especially during migration to the NPSBN.	N/A	SHALL		N/A
OH	FirstNet SHALL provide technical performance reports to user agencies on a per-sector basis.	N/A	SHALL		N/A
OH	FirstNet SHALL establish a single, nationwide common User Address format for the benefit of interoperable communications and incident management.	N/A	SHALL	<p><i>It would be very useful to be able to reference from a User Address information about the user including their personal identity, home agency, discipline. Users may go anywhere with their device; especially in response to major disasters.</i></p> <p><i>It would be very useful for every user to have the same User Address format in these cases.</i></p> <p><i>For example, if someone makes an emergency call, it would be very useful to be able to identify, from the User Address only, that the call is coming from a utility worker that is outside of their home jurisdiction.</i></p> <p><i>Also for example, when geofencing users within an incident to assign priority, it would be very useful to the dispatcher/IC to know from the User Address the same information covered above.</i></p> <p><i>On commercial networks, each market has its own ID. Users of that regional/local ID are able to roam anywhere.</i></p>	N/A
OH	The network SHALL support what appears to be full duplex to the user, regardless of network, application, or handset hardware to force half duplex for traffic optimization purposes.	N/A	SHALL	<i>First Responders often operate in environments with large amounts of ambient and background noise including sirens, weather, and crowds that might trigger mic sense for half duplex on conventional cell phones.</i>	N/A
OH	A PSE SHALL demonstrate that any individual being granted access to network control components for either monitoring or configuration purposes has completed a full background check; the background check is to be completed by the PSE or by a suitably authorized third party.	N/A	SHALL		N/A
OH	New Req: The NPSBN operator SHALL depict actual, verified, end-user experience (e.g., average throughput) on its depiction of current coverage.	N/A	SHALL		N/A
SOR	The NPSBN architecture SHALL provide transport between NPSBN O&M Services and a NPSBN EPC.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a NPSBN-U and non-home PSEN as needed.	SHALL	SHALL		Same
SOR	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	The NPSBN architecture SHALL provide transport between a NPSBN-U and NPSBN Services.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a NPSBN-U and NPSBN O&M Services.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a NPSBN-U and 9-1-1 call centers.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a NPSBN-U and another NPSBN-U attached to the same EPC.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a NPSBN-U and another NPSBN-U attached to a different EPC.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a NPSBN-U and a commercial roaming exchange.	SHALL	SHALL		Same

SOR	The nationwide private IP network SHALL support route diversity to provide public-safety grade reliability.	SHALL	SHALL		Same
SOR	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	The nationwide private IP network SHALL support power backup for public safety-grade level of continuous electricity outage.	SHALL	SHALL		Same
SOR	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	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	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	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	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	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	The NPSBN SHALL support local IP applications in the PSEN.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support transport of VPN traffic from an NPSBN-U to the PSEN.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support transport of prioritized traffic from/to the PSEN.	SHALL	SHALL		Same
SOR	NPSBN services SHALL be accessible directly from a NPSBN-U connected to the NPSBN by an authorized user.	SHALL	SHALL		Same
SOR	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	FirstNet SHALL size the connections to each PSEN in accordance with the SLA with the PSEN.	SHALL	SHALL		Same
SOR	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	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	NPSBN services SHALL be accessible from a PSEN by authorized users connected to the PSEN via any means.	SHALL	SHALL		Same
SOR	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	The NPSBN and NPSBN-U equipment SHALL support NPSBN-U mobility across the entire NPSBN.	SHALL	SHALL		Same
SOR	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	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	NPSBN-U SHALL have access to the Internet via NPSBN transport to access any Internet provided service or data.	SHALL	SHALL		Same
SOR	The NPSBN SHALL allow VPN access to data via the Internet transport.	SHALL	SHALL		Same
SOR	The NPSBN SHALL be protected against attack via the Internet access and PSEN's shall follow FirstNet security policies.	SHALL	SHALL		Same
SOR	User agencies SHALL have the option to block Internet access to their user devices.	SHALL	SHALL		Same
SOR	User agencies SHALL have the option to provide Internet access to their devices via their own agency Internet transport.	SHALL	SHALL		Same
SOR	Backhaul links SHALL be designed for high availability.	SHALL	SHALL		Same
SOR	Design of the backhaul SHALL account for traffic overloads, e.g., during large-scale events.	SHALL	SHALL		Same
SOR	Backhaul transmission delays SHALL support the end-to-end delay budgets established for latency-sensitive applications.	SHALL	SHALL		Same
SOR	Switchover time from a primary path to a redundant path SHALL be imperceptible to LTE-users.	SHALL	SHALL		Same
SOR	All backhaul and inter-connect sites SHALL be protected against loss of commercial power.	SHALL	SHALL		Same
SOR	Secure remote monitoring, configuration, troubleshooting, and reset of transport equipment SHALL be available at each node.	SHALL	SHALL		Same
SOR	The backhaul network SHALL be scalable to accommodate traffic growth.	SHALL	SHALL		Same
SOR	The NPSBN O&M solution SHALL provide provisioning and management of NPSBN Users (NPSBN-U).	SHALL	SHALL		Same
SOR	The NPSBN O&M solution SHALL provide access to detailed, current, and historical billing and usage information per Section 4.6.9.	SHALL	SHALL		Same
SOR	The NPSBN SHALL have the ability provide an alarm stream to each PSE, scoped to network/service outage-level events.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide a secure performance management interface scoped to the PSE.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide performance data scoped to the PSE.	SHALL	SHALL		Same
SOR	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	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	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	FirstNet SHALL implement a coverage and capacity expansion plan.	SHALL	SHALL		Same

SOR	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	Applications deployed by FirstNet SHALL support user addressing.	SHALL	SHALL		Same
SOR	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.	SHOULD	SHOULD		Same
SOR	As identified in the previous table, FirstNet SHALL enable PSE O&M Users to deploy the identified user services.	SHALL	SHALL		Same
SOR	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	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	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	The NPSBN SHALL support all three categories of CMAS alerts: Presidential, Imminent Threat, and Child Abduction/AMBER alerts.	SHALL	SHALL		Same
SOR	NPSBN-Us SHOULD be allowed to opt-out of the presentation of specific alerts that are not Presidential alerts.	SHOULD	SHOULD		Same
SOR	The NPSBN SHALL provide an application distribution and management service for NPSBN-U applications.	SHALL	SHALL		Same
SOR	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		Same
SOR	The NPSBN 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		Same
SOR	NPSBN devices SHOULD be capable of being shared amongst different authorized human users.	SHOULD	SHOULD		Same

SOR	The NPSBN SHALL support OTA Diagnostics Monitor (e.g., LTE radio statistics) management.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support a communication path between an agency's NPSBN-U's and the PSEN without imposing a NAT.	SHALL	SHALL		Same
SOR	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	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	<i>The methodology for what is an acceptable data and coverage factor will be identified by parallel OFIP deliverables; specifically, traffic models and service data.</i>	Same
SOR	Backhaul links SHOULD be engineered to distinguish (or segregate between) PSEN traffic from (and) secondary users traffic when applicable.	SHOULD	SHOULD		Same
SOR	The NPSBN-U SHALL have UEs that support FirstNet-approved minimum set of voice and video CODECs.	SHALL	SHALL		Same
SOR	Each PSE administrator SHALL have the ability to remove the authorization to access an application.	SHALL	SHALL		Same
SOR	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	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	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	Each PSE administrator SHALL have access to summary data that will show the progress on all tickets for the PSE and for those that they have initiated or those which relate to a specific user under their authority.	SHALL	SHALL		Same
SOR	Each PSE administrator SHALL have the ability to record in inventory, assign, and track devices in the local replacement pool.	SHALL	SHALL		Same
SOR	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	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	The NPSBN SHALL provide an O&M tool.	SHALL	SHALL		Same
SOR	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	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	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	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	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	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	NPSBN-Us SHOULD require UEs that can be completely disabled remotely (i.e., "kill") when compromised.	SHOULD	SHOULD		Same
SOR	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		Same
SOR	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	The NPSBN SHALL establish procedures for application owners to open required ports and protocols for access control/firewall traversal.	SHALL	SHALL		Same
SOR	The NPSBN SHALL inspect all network traffic at security boundaries for intrusions.	SHALL	SHALL		Same
SOR	The NPSBN SHOULD actively prevent intrusions.	SHOULD	SHOULD		Same
SOR	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	The NPSBN SHALL provide the ability to manually control access to the NPSBN for different classes of first responders.	SHALL	SHALL		Same
SOR	When an NPSBN-U receives an incoming call from a non-public safety system (e.g., peer IPbased 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	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	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	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	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	Should pre-emption be required, the NPSBN SHALL first pre-empt secondary user resources before pre-empting any resources used by a primary user.	SHOULD	SHOULD		Same
SOR	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	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	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	PSE network managers SHALL be able to view the real-time dynamic priority condition of all users under their authority.	SHALL	SHALL		Same
SOR	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	PSE network managers SHALL be able to modify the QoS role of users within their scope.	SHALL	SHALL		Same
SOR	FirstNet SHALL establish policies to provide user entities prompt trouble reports, information helpful to facilitate operations using contingency communications, and restoration reports.	SHALL	SHALL		Same
SOR	FirstNet SHALL implement policies and guidance to ensure common NPSBN use and support.	SHALL	SHALL		Same
SOR	FirstNet SHALL implement procedures for the activation, deployment, and deactivation of technical resources.	SHALL	SHALL		Same
SOR	FirstNet SHALL provide support for procurement of goods and services.	SHALL	SHALL		Same
SOR	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	Applications deployed by FirstNet SHALL support device addressing.	SHALL	SHALL		Same
SOR	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	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	The NPSBN SHALL allow authorized PSE O&M Users to configure which NPSBN user classes an NPSBN-U's calling address (e.g., telephone number) is shared. The intent of this requirement, for example, is to prevent the NPSBN-U's telephone number and addressing information from being shared with secondary users on the NPSBN. For example, federal users may only want to share their telephone number with other federal users. 'User classes' can be groupings such as 'primary users', 'secondary users', 'federal users', etc.	SHALL	SHALL		Same
SOR	After originating the NG9-1-1 session, NPSBN-U's SHALL be able to send to and receive from the local PSAP's NG9-1-1 system, emergency text messaging.	SHALL	SHALL		Same
SOR	After originating the NG9-1-1 session, NPSBN-U's 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	After originating the NG9-1-1 call, NPSBN-U's 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	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	The NPSBN SHALL be able to receive CMAS alerts from the CMAS Federal Alert Gateway.	SHALL	SHALL		Same
SOR	All NPSBN-U's SHALL be able to receive CMAS text alerts using CMAS-capable UE that can present the alert.	SHALL	SHALL		Same
SOR	NPSBN-U's SHALL have the capability to send and receive text messages to and from other NPSBN-U's and CN-U's.	SHALL	SHALL		Same
SOR	NPSBN-U's SHALL have the capability to send text messages addressed to a group of NPSBN-U's.	SHALL	SHALL		Same
SOR	NPSBN-U's SHALL have the capability to send and receive multimedia messages to and from other NPSBN-U's.	SHALL	SHALL		Same
SOR	NPSBN-U's SHALL have the capability to send multimedia messages addressed to a group of NPSBN-U's.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support the ability for a PSEN to deploy one or more video applications.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide the ability for one or more PSEs to stream video traffic in real-time to one or more other PSEs. The intent is to support the sharing of fixed and mobile video assets between PSEs.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide the ability for NPSBN-U's belonging to different PSEs to exchange real-time video streams from a PSEN-deployed video service.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide the ability for one or more NPSBN-U's to stream video traffic in real-time to one or more other NPSBN-U's using the NPSBN video service.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support the ability to interface with fixed video sources (including thirdparty systems), such as facility security cameras.	SHALL	SHALL		Same
SOR	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	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	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	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	** Any "immediate peril" feature is to be a SHALL NOT on the basis that there should be only one emergency call function.	Different

SOR	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	** Any "immediate peril" feature is to be a SHALL NOT on the basis that there should be only one emergency call function.	Different
SOR	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	** Any "immediate peril" feature is to be a SHALL NOT on the basis that there should be only one emergency call function.	Different
SOR	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 PSEs.	SHALL	SHALL		Same
SOR	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 PSEs based on the user of the UE.	SHALL	SHALL		Same
SOR	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	The NPSBN SHALL support Over-the-Air (OTA) SIM management.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support OTA Firmware Update management.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support OTA Software Configuration management.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support OTA APN connection management.	SHALL	SHALL		Same
SOR	NPSBN UE SHALL support dual stack IPv4/IPv6.	SHALL	SHALL	Essentially every device manufactured today runs dual-stack IP versions so this is not a particularly difficult requirement to meet.	Same
SOR	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	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	Each PSE administrator SHALL have the ability to change the authorized applications and their settings.	SHALL	SHALL		Same
SOR	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	FirstNet's security policy SHALL require applications and user services to be secure against intrusion.	SHALL	SHALL		Same
SOR	PSEN-hosted applications SHALL be allowed to use the NPSBN identity management system.	SHALL	SHALL	Assumes that the NPSBN has an identity management system AND provides cloud hosting.	Same
SOR	PSEN-hosted applications SHALL NOT be required to use the NPSBN identity management system.	SHALL NOT	SHALL NOT	Assumes that the NPSBN has an identity management system AND provides cloud hosting.	Same
SOR	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	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	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	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-U's. 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	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	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	The NPSBN SHALL provide near-real-time usage alerts to the PSEN and the initiating NPSBN-U's associated device(s) when any dynamic priority and QoS control described in this section has been activated or de-activated.	SHALL	SHALL		Same
SOR	NPSBN-U's 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	The information called Location Information SHOULD at a minimum include geographical location, time, date, and a unique identifier.	SHOULD	SHOULD		Same
SOR	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	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	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	SHOULD		Same
SOR	The network management service SHALL allow an authorized entity to retrieve a particular UE's current network location (RAN, eNodeB).	SHALL	SHALL		Same
SOR	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	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	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	An authorized PSEN administrator SHALL be able to configure which NPSBN-Us can initiate and clear the emergency condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the emergency condition.	SHALL	SHALL		Same
SOR	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	These DNS services, when provided, SHALL also be accessible from other public safety networks such as PSAPs.	SHALL	SHALL		Same
SOR	PSEs SHALL be actively notified of planned future changes in advance that may adversely affect their use of the network.	SHALL	SHALL		Same
SOR	PSEs SHOULD have a voice in approving DNS changes made to the NPSBN that have potential to adversely affect them.	SHOULD	SHOULD		Same
SOR	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	To allow for nimble recovery from NSPBN system failures and ensure public safety users with a simple roaming experience, DNS server IP addresses SHOULD NOT be hard coded in an individual UE.	SHOULD NOT	SHOULD NOT		Same
SOR	The NPSBN MUST put in place a system to ensure IP addresses across the entire national level of the FirstNet system are unique.	SHALL	SHALL		Same
SOR	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	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	The NPSBN SHALL provide a network time service available to NPSBN infrastructure.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide a network time service available to mobile users of the network.	SHALL	SHALL		Same
SOR	The identity management framework SHALL enable applications and services to securely verify the identity of users.	SHALL	SHALL		Same
SOR	The identity management framework SHALL be standards based.	SHALL	SHALL		Same
SOR	Identity assertions SHALL be cryptographically protected when being transmitted from one entity to another in the network.	SHALL	SHALL		Same
SOR	The identity management framework SHALL issue identities to non-person entities on the network.	SHALL	SHALL		Same
SOR	The identity management framework SHALL enable non-person entities to authenticate to applications and services where authorized.	SHALL	SHALL		Same
SOR	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	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	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	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	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	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	The NPSBN authentication services SHALL support industry standard authentication interfaces for mobile and fixed infrastructure components.	SHALL	SHALL		Same
SOR	The identity management framework SHALL manage privileges for person and non-person entities.	SHALL	SHALL		Same
SOR	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	The NPSBN architecture SHALL provide transport between a NPSBN-U and its home PSEN.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between NPSBN Services and a PSEN.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between NPSBN Services and NPSBN O&M Services.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between NPSBN Services and 9-1-1 call centers.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between NPSBN Services and the PSTN. (This is required if PSTN service is implemented at launch.)	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between NPSBN O&M Services and a PSEN.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a PSEN and commercial networks.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between a PSEN and a NPSBN EPC.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support access controls necessary to limit users from access to network control and signaling assets.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support the ability based on a users identity to limit or expand access to either shared or private services served locally, regionally, or nationwide including other PSEs.	SHALL	SHALL		Same
SOR	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	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	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	The NPSBN SHALL protect using encryption and access control the network signaling, configuration, and other control interfaces of the network.	SHALL	SHALL		Same
SOR	The NPSBN SHALL limit access by user, function, and on a need-to-know basis to network control components.	SHALL	SHALL		Same

SOR	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	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	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	The NPSBN SHALL have the ability to shut down any external interface or connection to roaming network if security threats are detected and determined to be a threat to NPSBN operations.	SHALL	SHALL		Same
SOR	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	The device management network service SHALL allow an authorized entity to install and enable malware/anti-virus protection.	SHALL	SHALL		Same
SOR	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	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	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	Suitably authorized PSE administrators SHALL be able to view a QoS configuration history for users under their authority.	SHALL	SHALL		Same
SOR	Suitably authorized PSE customer service representatives SHALL be able to view a QoS configuration history for users under their authority.	SHALL	SHALL		Same
SOR	The telephony service SHALL support the creation and use of dialing plans using short-address numbers. The intent is to allow NPSBN-U's 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	The NPSBN SHALL provide a presence service.	SHALL	SHALL		Same
SOR	The NPSBN architecture SHALL provide transport between CMAS and a NPSBN-U.	SHALL	SHALL		Same
SOR	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		Same
SOR	Backhaul transmission delays SHALL support the end-to-end delay budgets established for latency-sensitive applications.	SHALL	SHALL	<i>Latency introduced by: number of hops; quality of routing/switching equipment; transmission type (e.g. fiber, mW, copper), security</i>	Same
SOR	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	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	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	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	FirstNet SHALL develop a policy for the NPSBN that requires a nationwide standard for prioritization and QoS.	SHALL	SHALL		Same

SOR	FirstNet SHALL define the default priorities of all user classes on the NPSBN.	SHALL	SHALL		Same
SOR	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	The lowest network priorities SHALL be reserved for those users who lease the spectrum for commercial and/or personal use.	SHALL	SHALL		Same
SOR	FirstNet SHALL establish a policy to enable PSEs and PSEN applications to be accessed via the NPSBN.	SHALL	SHALL		Same
SOR	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	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	FirstNet SHALL establish a certification process for all network hardware and firmware.	SHALL	SHALL		Same
SOR	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	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	The NPSBN SHALL support future defined applications as required by PS Users and as sanctioned by FirstNet.	SHALL	SHALL		Same
SOR	FirstNet SHALL implement process-improvement procedures for roadmap management including feature-request and feature-prioritization processes.	SHALL	SHALL		Same
SOR	FirstNet SHALL plan and maintain budget items for upgrades and technology refresh according to the established roadmap.	SHALL	SHALL		Same
SOR	FirstNet SHALL implement an upgrade/maintenance coordination and notification process with all appropriate partners.	SHALL	SHALL		Same
SOR	FirstNet SHALL maintain backwards compatibility with deployed UEs as allowed by 3GPP standards.	SHALL	SHALL		Same
SOR	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	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	FirstNet SHALL establish a policy to schedule network maintenance.	SHALL	SHALL		Same
SOR	FirstNet SHALL establish a policy to notify users of scheduled maintenance that may impact the user experience on the NPSBN.	SHALL	SHALL		Same
SOR	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	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	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	The NPSBN SHALL support full-duplex telephone sessions between a mobile NPSBN-U and the PSTN.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support full-duplex telephone sessions between a mobile NPSBN-U and a commercial network user (CN-U).	SHALL	SHALL		Same
SOR	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-U's. For example, dialing restrictions to prevent 900-number calling.	SHALL	FALSE		Different
SOR	The NPSBN SHALL allow authorized PSE O&M Users to optionally block anonymous or private incoming calls to their associated NPSBN-U's.	SHALL	SHALL		Same
SOR	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	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	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	For telephony calls between two or more NPSBN-U's 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	The NPSBN shall support the transmission of telephony caller addressing information (e.g., "Caller ID").	SHALL	SHALL		Same
SOR	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	The telephone service SHALL support toll (or better) audio quality.	SHALL	SHALL		Same
SOR	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	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	The NPSBN shall support telephony voicemail service.	SHALL	SHALL		Same
SOR	On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the use of voicemail service.	SHALL	SHALL		Same
SOR	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	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	The NPSBN SHALL support telephony call conferencing.	SHALL	SHALL		Same
SOR	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	All NPSBN-U SHALL be able to receive CMAS text alerts using CMAS-capable UE that can present the alert.	SHALL	SHALL		Same
SOR	The NPSBN SHALL support the periodic testing of CMAS service as defined by the FCC.	SHALL	SHALL		Same
SOR	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	The NPSBN presence service SHALL provide interface specifications for use by other application servers.	SHALL	SHALL		Same
SOR	The NPSBN SHALL limit access to UE device location information based on PSE policies.	SHALL	SHALL		Same
SOR	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	The design of the NPSBN SHALL account for higher traffic demand in areas deemed strategic by FirstNet and/or PSEs.	SHALL	SHALL	<i>The methodology for how areas are deemed "strategic" is a substantial task addressed by parallel OFIP deliverables.</i>	Same
SOR	Coverage validation SHALL follow industry "best" practices.	SHALL	SHALL	<i>Coverage validation procedures shall be designed to meet Ohio's requirements as communicated to FirstNet through data collection activities, especially with consideration towards all applicable use environments (e.g., indoor, outdoor, handheld, mobile, etc). When determining coverage characteristics that we want to see, we need to acknowledge the community's standards.</i>	Same
SOR	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	FirstNet SHALL define the requirements for agencies and/or authorities to qualify as NPSBN users.	SHALL	SHALL		Same
SOR	NPSBN backhaul, transport, and IP packet prioritization techniques SHALL be consistently applied to the entire NPSBN.	SHALL			Not reviewed
SOR	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			Not reviewed
SOR	Backhaul links SHOULD be engineered to distinguish (or segregate between) PSEN traffic from (and) secondary users traffic when applicable.	SHOULD	SHALL	<i>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 MARCS. Informal poll is that MARCS is nearly 100% mobile.</i>	Different
SOR	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	<i>** Any "immediate peril" feature is to be a SHALL NOT on the basis that there should be only one emergency call function.</i>	Different
SOR	The NPSBN SHALL provide a user portal that allows a jurisdiction to configure new UEs with their specific information.	SHALL	SHALL	<i>Functionally equivalent to enterprise service from a carrier today.</i>	Same

SOR	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 NOT		Different
SOR	FirstNet SHALL implement a coverage and capacity expansion plan.	SHALL	SHALL	<i>Note; redundant to 11.2. See comments on SOR-11.2.</i>	Same
SOR	In conjunction with NPSBN service, a commercial cellular roaming agreement SHALL be offered.	SHALL	SHALL		Same
SOR	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	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	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	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	A commercial cellular system to NPSBN transition test plan SHALL be provided to assist migration to the NPSBN.	SHALL	SHALL		Same
SOR	FirstNet SHOULD develop a policy defining the ability and process for local, tribal, state, and federal entities to monitor the network.	SHOULD	SHALL	<p><i>For MARCS; only entities that share a zone controller have any visibility into the network. E.g. Jefferson County, Butler County, Lake County.</i></p> <p><i>On MARCS, local users receive automatic statistical reports. They can also sign up for email notifications about network troubles.</i></p> <p><i>There is little justifiable need for end user agencies to actively monitor the network.</i></p> <p><i>However, there must be a policy providing for which network information, protocols and/or interfaces agencies may monitor (if any), and if so, how they can get access to the information.</i></p>	Different
SOR	FirstNet SHALL establish a policy to provide user entities insight into overall system performance metrics, including availability and coverage.	SHALL	SHALL	<i>Must also include: Peak and average user density per sector; Peak and average throughput.</i>	Same
SOR	FirstNet SHALL establish standardized training programs to deliver to all personnel who manage NPSBN communications resources.	SHALL	SHALL	<p><i>Lessons from MARCS: Standardized training materials, including visual aids and talking points.</i></p> <p><i>MARCS staff will perform end-user and TTT on request for end-user agencies covering basic features of the radio and how to use it as well as interoperability requirements and features.</i></p> <p><i>When MARCS first arrived at sheriff's offices, MARCS provided initial training but also provided an operations manual.</i></p> <p><i>The NPSBN will almost certainly have standardized interoperability applications and/or interfaces unique to the NPSBN. FirstNet should provide training resources in these areas, for example.</i></p> <p><i>Based on this experience, agencies that FirstNet has some sort of training program.</i></p>	Same

SOR	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	<i>It is infeasible for FirstNet to provide formal training for all agencies, disciplines and jurisdictions.</i> <i>Per 18.1, agencies will expect TTT programs, standardized training materials, and/or self-paced learning provided by FirstNet.</i>	Same
SOR	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	SHALL	SHALL	<i>If a public safety entity has the ability to log content, that entity may then be held liable for the data.</i> <i>Agencies have historically been responsible for reproducing their communications records and other data.</i> <i>Foreseen issue: Body cam footage; which retention schedule is it held to? It is a large amount of footage; how is stored and transported.</i>	Same
SOR	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	<i>Subject to classification of data types; QoS parameters on FirstNet's network</i>	Same
SOR	Encrypted NPSBN application content SHALL NOT be decrypted prior to transfer to the PSEN.	SHALL NOT	SHALL NOT	<i>A shared key environment is inherently insecure; makes this feasible for one-to-many traffic; somewhat dependent on PKI</i> <i>Traffic is encrypted over the air; it is not encrypted on the wired network.</i> <i>Essentially, this requirement enforces end-to-end encryption.</i>	Same
SOR	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	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		Same
SOR	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	<i>Workgroup assumes that this requirement provides that multimedia is buffered somewhere in the network.</i>	Same
SOR	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	<i>Time zone can be determined by the user location; it is not really relevant to the requirement.G304</i> <i>Logging content muse also include content source application identity, if known or available; QoS classification, esp. if application identity is not known.</i> <i>Assuming end-to-end QoS, even for encrypted content, the data type will be identified in a container header; therefore, we can identify the QoS classification.</i>	Same

SOR	The NPSBN SHALL maintain logging usage records identifying which PSE O&M User activated or de-activated the logging service.	SHALL	SHALL		<i>Comment: Better language: system shall provide vs. system shall maintain</i>
SOR	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	STRIKE	<i>This requirement is not practiceable; there will be different devices, OSes, form factors, etc.</i> <i>The practicalities of putting such a system into use--including version control for all hardware on the network, managing device images for on-demand delivery and delivering application installation files, updates, patches and drivers over the network--are not feasible.</i>	Different
SOR	For applications deployed by FirstNet, it SHALL be possible for the receiving NPSBN-U to identify the user address of the content source. This requirement may not be readily achievable should the call or session originator be a non NPSBN-U.	SHALL	SHALL		Same
SOR	For applications deployed by FirstNet, a common User Address format SHOULD be created. The intent is to define a consistent identification format.	SHOULD	SHALL		Different
SOR	As identified in the previous table, FirstNet SHALL provide the identified user services to NPSBN-Us.	SHALL	SHALL	<i>Refer to SOR-23 for the table in question.</i> <i>Interoperable public safety grade video is a "killer app" for the NPSBN; per FN Special Notice, video features start to become available in IOC-2 and 3 (6 months-2 years)</i>	Same
SOR	The NPSBN SHOULD support full-duplex telephone sessions to devices.	SHOULD	SHALL	<i>Distinction between full-duplex and half-duplex that appears to be full-duplex to the user.</i>	Different
SOR	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	The messaging service SHALL provide a standard mechanism to provide interoperability with PSEN email systems. The intention is for the messaging service to provide a standard mechanism (e.g., SMTP) to allow for message interoperability with PSEN email systems as opposed to supporting many such interfaces.	SHALL	SHALL		Same
SOR	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	<i>Should be implemented via an SMS gateway, much like xyz@txt.att.net.</i>	Same

SOR	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	<i>Should be implemented by an MMS gateway, e.g. xyz@mms.att.net.</i>	Same
SOR	The information content of NPSBN Status Web Pages SHALL be accessible for both reading and writing by applications.	SHALL	SHALL	<i>Workgroup assumes only suitably authorized O&M users can read/write Status Web Pages.</i>	Same
SOR	The NPSBN SHOULD provide application hosting capabilities within the NPSBN.	SHOULD	SHOULD	<i>Workgroup assumes based on this requirement that FirstNet should be a cloud hosting provider.</i>	Same
SOR	PSEs SHALL NOT be required to host applications within the NPSBN Services.	SHALL NOT	SHALL NOT	<i>Assuming FirstNet provides hosting services.</i>	Same
SOR	PSEs SHALL be able to locally host applications within the agency PSEN.	SHALL	SHALL		Same
SOR	The NPSBN SHOULD provide a service hosting platform as a service to PSEs.	SHOULD	SHOULD	<i>Assuming FirstNet provides hosting services.</i>	Same
SOR	The NPSBN SHALL provide the ability for PSEs to remotely manage their applications.	SHALL	SHALL	<i>Assuming FirstNet provides hosting services.</i>	Same
SOR	The NPSBN SHOULD provide a service hosting platform as a service to vendors.	SHOULD	SHOULD	<i>Assuming FirstNet provides hosting services; there could be a lot of benefit to a vendor hosting public safety applications natively within the NPSBN cloud architecture. For example, a CAD vendor could more easily provide a high level of security and interoperability if all of the data resides in the NPSBN.</i>	Same
SOR	The NPSBN SHALL provide the ability for vendors to remotely manage their applications.	SHALL	SHALL	<i>Assuming FirstNet provides hosting services.</i>	Same
SOR	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		Same
SOR	Intra-NPSBN handover SHALL NOT be perceptible to the user.	SHALL NOT	SHALL NOT		Same
SOR	The use of standard-compliant high-power NPSBN UEs SHALL NOT create harmful interference to any UEs' NPSBN services.	SHALL NOT	SHALL NOT		Same
SOR	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	The NPSBN SHALL be designed according to measurable GoS levels throughout the NPSBN service area.	SHALL	SHALL	<i>Refer to 17.3 for GoS measurements.</i>	Same
SOR	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	The required data throughput performance of applications SHALL be maintained at vehicular speeds.	SHALL	SHALL		Same
SOR	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	STRIKE	<i>There is no reasonable expectation that this requirement is achievable if secondary users are allowed on the network. For secondary user requirements, see SOR-119.</i> <i>Any addition to the network will, in some way, affect the performance of every other user. E.g., if there is an incident at site 1 sector A, and that site shares backhaul with sites 2, 3, 4, and 5, secondary users on sites 2-5 may contribute to congestion on shared backhaul which will affect the experience for users at the incident site.</i> <i>Some secondary users will occasionally qualify as primary users during incidents, e.g. utilities. The service must accommodate the scenario where a user, who is normally a secondary user, may be elevated to primary public safety status.</i>	Different

SOR	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	<i>A Line includes most of northern 1/3 of Ohio; international coordination is a US-Canada treaty issue.</i> <i>Allen County case study: had to coordinate frequency internationally through Industry Canada. Eventually moved antenna south of the A line.</i>	Same
SOR	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	SHOULD	<i>There is no reasonable expectation when roaming off of BC14 that a user would have anything other than best-effort service; when the user is on a commercial network, they should expect commercial service.</i> <i>By "SHOULD" the workgroup means that FirstNet should endeavor to secure a higher grade of service through its commercial roaming partner; e.g., priority access without ruthless pre-emption or guaranteed bandwidth; such features would make FN's offer favorable compared to commercial services.</i> <i>Significance: As a "should", we are saying that we would LIKE an SLA with FN's roaming partner, but do not require it.</i> <i>The premise for FN: commercial carriers provide best-effort service and they support FirstNet because their business is not designed to support mission-critical service.</i> <i>If future regulations require commercial carriers to provide mission-critical service, then Ohio would change this requirement to a SHALL.</i>	Same
SOR	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	The NPSBN SHALL support capacity and/or coverage expansion to address evolving users needs.	SHALL	SHALL	<i>The methodology for how "evolving user needs" are determined and met will be identified by parallel OFIP deliverables.</i>	Same
SOR	FirstNet SHALL provide coverage in the service area(s) required by PSE.	SHALL	STRIKE	<i>The methodology for what is considered "required coverage by PSE" will be identified by parallel OFIP deliverables and FN data collection efforts.</i>	Different
SOR	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	STRIKE	<i>OFIP program and FirstNet consultation are investing substantial effort into each individual agency's coverage requirements throughout the state; therefore this requirement does not apply as it is redundant and it does not say enough about user coverage needs.</i>	Different
SOR	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	The RF planning and design of the NPSBN SHALL account for the possible coexistence of standard-compliant low and high-power UEs.	SHALL	SHALL	<i>As emerging standards allow.</i>	Same
SOR	The NPSBN infrastructure's availability SHALL be typical of a public-safety grade network.	SHALL	SHALL	<i>When providing service to cellular towers, carriers usually require redundant routes to each tower; most commercial towers throughout rural OH have redundant fiber links.</i> <i>For MARCs system: fiber where practical, otherwise mW; goal: fiber and mW to every tower.</i>	Same
SOR	Issues impacting availability SHALL be managed within agreed SLAs.	SHALL	SHALL	<i>Workgroup members expect an SLA from FirstNet.</i>	Same
SOR	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	<i>Proposed requirements: within 24-48 hours for emergencies; as-needed for pre-planned incidents;</i> <i>NIMS: Initial planning window is 12 hours; therefore it is reasonable to expect deployables within second operational period, or 12-24 hours</i> <i>E.g.: MARCS has three towers on wheels. Buckeye State Sheriff's Association has multiple communications vehicles available on an as-needed basis that include cache radios and gateways/patching devices.</i>	Same
SOR	Service restoration time following an outage SHALL be minimal as per a service level agreement.	SHALL	SHALL		Same
SOR	Scheduled maintenance SHALL have minimal impact on services.	SHALL	SHALL		Same

SOR	Silent failure modes, i.e., failed backup components that have gone undetected, SHALL be minimized.	SHALL	SHALL		Same
SOR	The network SHALL revert to its original state of operation upon failure resolution.	SHALL	SHALL		Same
SOR	Adequate spare parts, antennas, transmission lines SHALL be stocked by the servicing agency.	SHALL	SHALL		Same
SOR	Remote reset of RAN equipment SHALL be available at each site.	SHALL	SHALL		Same
SOR	Any redundant NPSBN core SHALL support the full RAN traffic load.	SHALL	SHALL		Same
SOR	Shelters housing NPSBN equipment SHALL be hardened according to best practices employed in the region.	SHALL	SHALL		Same
SOR	NPSBN-US SHOULD have consumer-equivalent smartphones capable of operating on both commercial networks and the NPSBN.	SHOULD	SHALL	<i>Per other requirements, FirstNet will have a very hard time achieving sustainability without market-leading cell phone platforms; as of this writing, iOS and Android that operate on both commercial networks and the NPSBN.</i>	Different
SOR	NPSBN-US SHOULD have consumer-equivalent tablet PCs capable of operating on both commercial networks and the NPSBN.	SHOULD	SHALL	<i>Per other requirements, FirstNet will have a very hard time achieving sustainability without market-leading cell phone platforms; as of this writing, iOS and Android that operate on both commercial networks and the NPSBN.</i>	Different
SOR	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 AS AMMENDED	<i>Strike: "that meet public safety requirements for in-vehicle installation"; it is not a meaningful requirement.</i> <i>Workgroup feels it is fair to require vehicle modems to operate on NPSBN and commercial networks because BC14 vehicular modems on the market today already do; further, as commercial roaming is a requirement, all devices must support both bands.</i>	Different
SOR	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	SHOULD	<i>Workgroup feels it is very unlikely many agencies will share a single smartphone or tablet between multiple users; device sharing is common in radio based on the cost of the device and a user experience that is conducive to device sharing.</i> <i>Workgroup also feels that multiple personality features built into devices specifically for the NPSBN may make the devices more specialized and expensive for a feature with very limited value.</i> <i>However, there are limited cases where the workgroup feels this feature may be useful and sees it as a low-priority, value-added feature.</i>	Same
SOR	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	NPSBN UE SHOULD support enhanced autonomous location services (e.g., latitude, longitude).	SHOULD	SHALL	<i>Location services are essential and widely used by all public safety organizations and consumers. There is no reason NPSBN UE should not be required to support this feature.</i>	Different
SOR	NPSBN UE SHOULD operate at power levels to meet the NPSBN coverage needs.	SHOULD	SHOULD	<i>Workgroup registers its concerns that high power levels may offer reduced battery life and are not likely to be necessary in urban areas.</i>	Same
SOR	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	Each PSE administrator SHALL have the ability to define the types of devices the user is authorized to use.	SHALL	SHALL		Same
SOR	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	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	The NPSBN Billing Interface SHALL provide commercial and application level integration capability.	SHALL	SHALL		Same
SOR	The NPSBN Billing Interface SHALL supply an interface for PSEs to query up-to-date billing detail at will.	SHALL	SHALL		Same
SOR	A PSE O&M administrator SHALL have the ability to add devices quickly and efficiently without coordination with others.	SHALL	SHALL		Same
SOR	A PSE O&M administrator SHALL have the ability to configure the device remotely.	SHALL	SHALL		Same

SOR	A PSE O&M administrator SHALL have the ability to push software upgrades/updates.	SHALL	SHALL		Same
SOR	A PSE O&M administrator SHALL have the ability to install additional applications.	SHALL	SHALL		Same
SOR	A PSE O&M administrator SHALL have the ability to control access to the device.	SHALL	SHALL		Same
SOR	A PSE O&M administrator SHALL have the ability to authenticate users.	SHALL	SHALL		Same
SOR	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	A PSE O&M administrator SHALL have the ability to remove applications and/or deactivate device applications.	SHALL	SHALL		Same
SOR	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	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	Public Safety Users, Secondary Users, and Application Users SHALL have the ability to enable Wi-Fi and Bluetooth features as required.	SHALL	SHALL	<i>Workgroup assumption: "as required" means "as required by the user".</i>	Same
SOR	The NPSBN SHALL support public safety applications, either by providing subscribers a means of connecting to their home PSEs, or by providing common nationwide applications, or both.	SHALL	SHALL		Same
SOR	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	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	<i>Shall be included in SLA; do not currently receive notice from carriers</i>	Same
SOR	The RAN, EPC, and transport equipment SHALL support capabilities to add redundant components while minimizing out-of-service time.	SHALL	SHALL	<i>Shall be included in SLA</i>	Same
SOR	The NPSBN location service SHALL provide location information associated with NPSBN users.	SHALL	SHALL	<p><i>Agencies expect to have access to the location service information for the devices and/or authenticated users in that agency's fleet and only that agency's fleet, unless authorized.</i></p> <p><i>Assumption: Applies to all entities acting as public safety users or in support of public safety users.</i></p> <p><i>Note: NPSBN users have no reasonable expectation of privacy of their location, subject to local policy protections, when in possession of an NPSBN-capable device.</i></p> <p><i>Note: E.g. Akron, AVL: Only available for safety and protection of officers; generally off-limits for IA; location history is not available to the public unless part of a formal records request</i></p>	Same
SOR	The NPSBN location service SHALL support authorization for access to NPSBN users' location information.	SHALL	SHALL		Same
SOR	NPSBN-U location information SHALL be available to PSEN hosted applications	SHALL	SHALL		Same
SOR	NPSBN-U location information SHALL be available to applications hosted via NPSBN Services.	SHALL	SHALL		Same
SOR	The NPSBN location service SHALL support strong security between location clients and servers.	SHALL	SHALL		Same
SOR	The NPSBN location service SHALL support receiving location information from NPSBN users while roaming.	SHALL	SHALL		Same

SOR	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	FirstNet SHALL define an NPSBN security policy for monitoring, logging, and data retention policies for NPSBN applications and services.	SHALL	SHALL		Same
SOR	FirstNet SHALL define a policy to insure that the NPSBN SHALL support capabilities to respond, in near real-time, to security threats without incurring a service outage.	SHALL	SHALL		Same
SOR	FirstNet SHALL define a policy to insure that updates to security management will not compromise existing security measures.	SHALL	SHALL		Same
SOR	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	The RAN, EPC, and transport equipment SHALL support capabilities to respond, in near realtime, to security threats.	SHALL	SHALL		Same
SOR	Updates to security management SHALLNOT compromise existing security measures.	SHALL	SHALL		Same
SOR	Applications hosted on the NPSBN SHALL comply with all NPSBN information assurance procedures, policies, and requirements.	SHALL	SHALL		Same
SOR	PSEs SHALL be allowed to provide additional layers of security if desired.	SHALL	SHALL		Same
SOR	FirstNet's security policy for user services and NPSBN-hosted applications SHALL require users to securely authenticate for access.	SHALL	SHALL		Same
SOR	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	FirstNet's security policies SHALL require applications hosted in PSEs to comply with clearly documented security policies and procedures designed to protect PSE and NPSBN infrastructure from cyber attack, loss, or exposure of sensitive information.	SHALL	SHALL		Same
SOR	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	The NPSBN SHALL protect user services infrastructure against corruption or unauthorized modification (e.g., software, configurations, etc.).	SHALL	SHALL		Same
SOR	The NPSBN SHALL periodically verify that the user services infrastructure and hosted applications servers do not present security vulnerabilities.	SHALL	SHALL		Same
SOR	NPSBN user services SHALL meet public safety-grade availability and reliability requirements.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide user services and applications hosted on the NPSBN access to the NPSBN identity management framework.	SHALL	SHALL		Same
SOR	NPSBN user services and applications SHALL use the NPSBN identity management system.	SHALL	SHALL	<i>Assumes that the NPSBN has an identity management system.</i>	Same
SOR	NPSBN-hosted agency applications SHALL use the NPSBN identity management system.	SHALL	SHOULD	<i>Assumes FirstNet offers a cloud hosting service. There is value in a large number of public safety agencies sharing a common identity management system. However, it is unlikely that many agencies will want to use FirstNet's cloud hosting if they are forced to migrate to a new IAM.</i>	Different
SOR	The NPSBN SHALL permit the use of last-used credentials to allow the set up of emergency calls without due course to the usual authentication process.	SHALL	SHALL		Same
SOR	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	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	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	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	<i>Workgroup observation: This would apply in addition to any civil or criminal penalties related to malicious use or tampering with the public safety network.</i> <i>Note: The NPSBN may require new laws in this area.</i>	Same
SOR	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	NPSBN-Us SHALL be authenticated prior to accessing the text and multimedia messaging service.	SHALL	SHALL		Same
SOR	NPSBN-Us SHALL be suitably authorized prior to accessing the text and multimedia messaging service.	SHALL	SHALL		Same
SOR	The messaging service SHALL provide confidentiality for text and multimedia messaging (both message content and related control).	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide the capability to filter spam and other undesirable text and multimedia messages as per configured policy.	SHALL	SHALL		Same
SOR	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	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	The messaging service SHALL have the ability to "whitelist" messaging contacts.	SHALL	SHALL		Same
SOR	The messaging service SHALL have the ability to "blacklist" messaging contacts.	SHALL	SHALL		Same
SOR	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	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	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	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		Same
SOR	The NPSBN SHOULD provide a status and information interface to the PSE administrators in a locality or agency responsible for a PSEN that any particular boundary device is between.	SHOULD	SHOULD		Same

SOR	The NPSBN SHALL have the ability to alert any PSEs, NPSBN-U, or PSEs of illegal, inappropriate, or problematic boundary activities.	SHALL	SHALL		Same
SOR	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	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	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	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	The NPSBN SHALL consider all UEs as untrusted and shall enforce security policies that protect NPSBN assets from UEs.	SHALL	SHALL		Same
SOR	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	The NPSBN SHOULD notify the appropriate agency or locality of any rogue device or devices deemed improper allocated to that agency PSEN.	SHOULD	SHOULD	<i>Individual agencies may prefer to be responsible for tracking rogue devices rather than depending on FirstNet to monitor and alert the agency.</i>	Same
SOR	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-U.	SHALL	SHALL		Same
SOR	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	<i>This is common best practice for enterprise networks; e.g., it is like connecting to your enterprise VPN and being subject to web filtering.</i>	Same
SOR	The NPSBN SHALL allow PSEs 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	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		Same
SOR	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	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	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	The NPSBN SHALL have a set of tools for analyzing and monitoring system and user log data to determine possible threats to the network before they occur or to support post-event activities.	SHALL	SHALL		Same
SOR	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	SHOULD	<i>FirstNet operating a validation service would be an added benefit, but workgroup members felt it is not an absolute requirement and would not fulfill an unmet need.</i>	Different

SOR	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	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 AS AMMENDED	<i>Trend in public safety organizations is to civilianize technical staff. Individual staff may or may not have completed a thorough background check prior to being franted PSEN O&M status.</i>	Different
SOR	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	<i>Scenario where the communication capability of the device is disabled, but the device location service is still active.</i>	Same
SOR	The NPSBN SHALL provide for an authorized entity to permanently remove a UE's ability to access the NPSBN.	SHALL	SHALL		Same
SOR	The device management network service SHALL allow an authorized entity to temporarily remove a UE's ability to access the NPSBN.	SHALL	SHALL		Same
SOR	The NPSBN SHALL provide the ability to lock out NPSBN UEs on commercial carrier networks.	SHALL	SHALL		Same
SOR	FirstNet SHALL be responsible for defining a minimum Information Assurance level for PSENs that wish to connect to the NPSBN.	SHALL	SHALL		Same
SOR	FirstNet SHALL use appropriate mechanisms to secure and protect user, management, and control plane traffic.	SHALL	SHALL		Same
SOR	All links between the PSEN and the NPSBN SHALL be properly protected by FirstNet if they traverse insecure domain/area.	SHALL	SHALL		Same
SOR	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		Same
SOR	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		Same
SOR	The NPSBN VPN capability, if provided, SHALL support VPN clients that are compatible with deployed and supported operating systems.	SHALL	SHALL		Same
SOR	User agencies SHALL be permitted to provide their own VPN solutions for accessing their PSEN.	SHALL	SHALL		Same
SOR	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		Same
SOR	The NPSBN SHALL implement access controls/firewalls to prohibit unallowed network connections and traffic.	SHALL	SHALL		Same
SOR	The NPSBN SHALL inspect all network traffic as possible based upon encryption level at security boundaries for malware and viruses.	SHALL	SHALL	<i>FirstNet will have very limited visibility into the contents of any encrypted traffic.</i>	Same
SOR	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		Same
SOR	Backhaul equipment SHALL be compliant with applicable standards and regulatory mandates.	SHALL	SHALL		Same
SOR	The NPSBN SHALL maintain a status of network security accessible by PSEN security personnel.	SHALL	SHALL		Same
SOR	Physical security of sites SHALL prevent unauthorized access.	SHALL	SHALL		Same
SOR	Local PSEN O&M administrators SHALL be provided with means to monitor alarms in their respective service area.	SHALL	SHALL		Same

SOR	Outdoor radio sites SHALL be equipped with physical and/or electronic means to detect, monitor, and deter unauthorized entry.	SHALL	SHALL	<p><i>This requirement to mean that NPSBN radio sites shall have a reasonable and cost-effective standard of physical security.</i></p> <p><i>For example, all MARCS sites are fenced and padlocked and use smart keys to keep track of who enters the building. Each site has a door alarm. There are cameras at some sites that are at high risk of theft or vandalism.</i></p> <p><i>Note: Some LTE sites, including micro and picocells, may have a relatively low level of physical security.</i></p>	Same
SOR	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	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-U's.	SHALL	SHALL		Same
SOR	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	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	The NPSBN SHALL distinguish between devices from public safety and secondary users during congestion to allow priority access for first responders if needed.	SHALL	SHALL		Same
SOR	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	<p><i>Workgroup assumes that secondary users who are cut off from the NPSBN at an incident will migrate to a commercial network.</i></p>	Same
SOR	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	<p>The NPSBN SHALL support the following relative application priorities when computing the NPSBN-U's default admission priority (1 = highest relative priority):</p> <ol style="list-style-type: none"> 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	N/A	<p><i>What is the highest priority service is highly dependent on the incident; e.g., in a school shooting incident video from cameras inside may be as or even more important than voice communications.</i></p> <p><i>Best practice network management practice is to place real-time multimedia as top priority.</i></p> <p><i>Priotization of traffic is a much more complicated topic than we can address in a single requirement in our table.</i></p> <p><i>This requirement does not add value on its own; assignment of priority is going to circumstantial.</i></p>	Different



Appendix 4: OFIP User Population Survey Preliminary Results

Provided below are snapshots from the Ohio Phase 2 Data Collection effort. This is a very limited subset from the total amount of data collected, and is provided as a guide to provide context to statements made earlier in the filing; in particular as our comments pertain to incumbent cellular provider coverage and user satisfaction with their commercial service.

While the full service includes nearly 100 questions, we have selected from only a small subset of responses to provide context and support for our assertions about coverage and incumbent cellular carriers.

Data Source

This data comes from our User Population Survey, which is part of the OhioFirst.Net Implementation Project and the NTIA State and Local Implementation Grant Program. As of this writing, we have 173 complete responses to our User Population Survey out of a total estimated 1000 responses by Q3 2016. This data represents a snapshot in time, and is a good indication of final results, but is not fully complete at this time.

Barriers to Adoption

We queried our users about barriers to adoption, asking whether cost, coverage, network performance, security, user expertise or perceived usefulness were barriers to the uptake of data. We specifically asked, “Which of the following factors have inhibited your adoption of wireless data services? Meaning, which of the following factors have led to you spending less on wireless data than you would otherwise?”

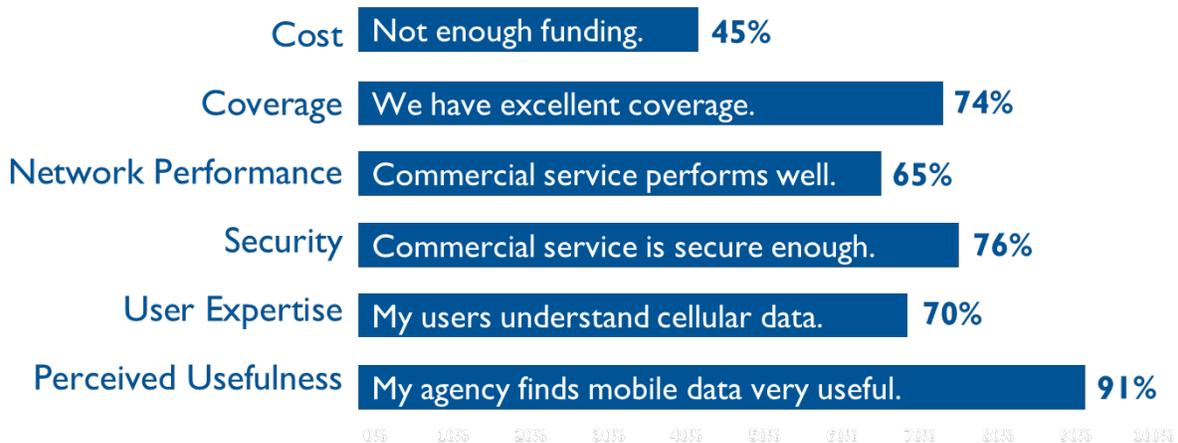


Figure 4: Barriers to Adoption of Commercial Wireless Service

Cost was the only significant barrier reported—however, the most common response was not “the monthly cost is too high”, but rather “the cost is fair, but my agency doesn’t have enough funding”. Survey respondents report being generally very satisfied with their commercial cellular service, reporting that it performs well (65%), provides excellent coverage (74%) and that they find great utility



in using mobile data (91%). These responses reinforce our position that FirstNet should set its baseline based on commercial wireless service—users feel that commercial networks are secure, perform well and provide sufficient coverage and will require that FirstNet’s network performs at least as well.

Current Carriers

In setting FirstNet’s baseline against commercial wireless service, it is important for FirstNet to understand which commercial carrier to set its baseline against. While we will identify which carrier each county and major city utilizes during our county-by-county coverage reviews, we have queried in our User Population Survey which commercial wireless carrier each respondent uses. Verizon is by far the most popular wireless carrier among public safety agencies in the state (63%) followed by AT&T (20%) and Sprint (19%).

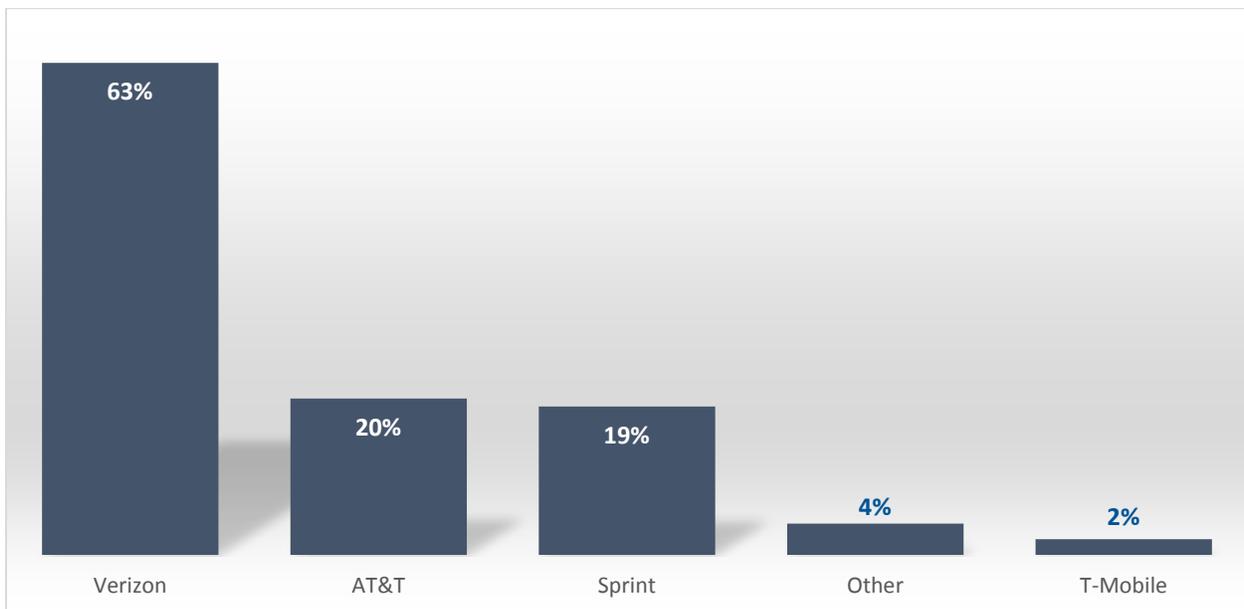


Figure 5: Current Commercial Carrier