SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE 1 OF PAGES

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NUMBER
	D15PS00295	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)		

7. ISSUED BY	CODE	8. ADDRESS OFFER TO *(If other than item 7)*
DEPARTMENT OF THE INTERIOR Acquisition Services Directorate ATTN: Gregory Ruderman, 703-964-3590, greg_ruderman@ibc.doi.gov		ATTN: Gregory Ruderman, Contracting Officer DOI, AQD/FirstNet 12200 Sunrise Valley Drive, Suite 100, Reston, VA 20191-3402

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and _____ copies for furnishings the supplies or services in the Schedule will be received at the place specified in item 8, or if hand carried, in the depository located in _____ until _____ *(Hour)* local time 05/31/2016 *(Date)*

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)* AREA CODE	NUMBER	EXTENSION	C. E-MAIL ADDRESS
	Stephanie Leikach	703	9648432		Stephanie_Leikach@ibc.doi.gov

11. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
☒	A	SOLICITATION/CONTRACT FORM	1	☒	I	CONTRACT CLAUSES	
☒	B	SUPPLIES OR SERVICES AND PRICES/COSTS				PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
☒	C	DESCRIPTION/SPECS./WORK STATEMENT		☒	J	LIST OF ATTACHMENTS	
☒	D	PACKAGING AND MARKING				PART IV - REPRESENTATIONS AND INSTRUCTIONS	
☒	E	INSPECTION AND ACCEPTANCE		☒	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
☒	F	DELIVERIES OR PERFORMANCE					
☒	G	CONTRACT ADMINISTRATION DATA		☒	L	INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS	
☒	H	SPECIAL CONTRACT REQUIREMENTS		☒	M	EVALUATION FACTORS FOR AWARD	

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 270 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232-8)*	10 CALENDAR DAYS (%)	20 CALENDAR DAYS (%)	30 CALENDAR DAYS (%)	CALENDAR DAYS(%)

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFER-OR	CODE	FACILITY	16. NAME AND THE TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*

15B. TELEPHONE NUMBER AREA CODE	NUMBER	EXTENSION	☐ 15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION

22. AUTHORITY FOR USING OTHER THAN FULL OPEN COMPETITION: ☐ 10 U.S.C. 2304 (c) ☐ 41 U.S.C. 3304(a) ( )	23. SUBMIT INVOICES TO ADDRESS SHOWN IN *(4 copies unless otherwise specified)*	ITEM

24. ADMINISTERED BY *(If other than Item 7)*	25. PAYMENT WILL BE MADE BY	CODE

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA	28. AWARD DATE
GREGORY RUDERMAN	*(Signature of Contracting Officer)*	

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

Table of Contents

List of Tables

B Supplies or Services and Prices/Costs

This Request for Proposal (RFP) is being issued by the Department of the Interior, Interior Business Center, Acquisition Services Directorate on behalf of the Department of Commerce, National Telecommunications and Information Administration (NTIA), First Responder Network Authority (FirstNet). This particular contract will provide for a single interoperable Nationwide Public Safety Broadband Network (NPSBN) as specified in Section C, Statement of Objectives (SOO), and the associated Section J attachments.

This competitive RFP is issued in accordance with Federal Acquisition Regulation Part 15 (Contracting by Negotiation). This is a full and open competition.

The Offeror shall furnish a comprehensive solution to meet the objectives as stated in the SOO and associated Section J attachments to include all personnel, materials, services, facilities, management, and other resources necessary to perform the objectives as set forth in the resultant contract. The comprehensive solution shall be described in a Performance Work Statement and Quality Assurance Surveillance Plan, see Section J, Attachment J-6, as a result of this RFP.

If interested in this acquisition, please participate in accordance with the instructions contained herein. Offerors will not be reimbursed for any costs incurred in developing their submission in response to this RFP.

The pricing structure for the Indefinite Delivery/Indefinite Quantity (IDIQ) contract will consist of the prices provided in the awarded pricing worksheets (see Section J, Attachment J-13, Pricing Template). The price structure is composed of two types of payments—payments to the Contractor and payments to FirstNet. Payments to the Contractor will draw down the budget authority described in Section B.4.1, Budget Authority. Payments to FirstNet will be supplied by the Contractor to ensure the ongoing financial sustainability of FirstNet, as described in Section B.4.4, FirstNet Operational Sustainability.

B.1 Price and Payment Redetermination

Price redetermination may occur should the Contractor determine a price adjustment for unit prices of supplies or labor and materials stated in the contract may be necessary. In this scenario, the Contractor shall submit a written request to the Contracting Officer identifying the rationale and justification for any adjustment and/or redetermination. Should the Contracting Officer determine an adjustment is appropriate, any such adjustment will be accomplished in accordance with the Federal Acquisition Regulation (FAR) economic price adjustment clauses (FAR 52.216-2, Standard Supplies, and FAR 52.216-4, Labor and Material) and/or FAR 52.216-5, Price Redetermination – Prospective Clause, as appropriate.

Periodic redetermination of the payments to FirstNet may be considered in accordance with the guidance provided herein, subject to the contract ceiling established herein. In no event shall the total amount paid under this contract exceed any ceiling price included in the contract unless otherwise modified.

The total amount of payments to FirstNet shall be proposed for all 56 states and territories. Should a particular state notify FirstNet of its intention to undertake responsibility for the RAN deployment and

operation pursuant to Section 6302 of the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), it must fulfill several other statutory obligations before it may deploy the RAN. Specifically, these states are required to meet specific statutorily required approval criteria as adjudicated by the Federal Communications Commission (FCC) and NTIA, as well as negotiate the terms of and enter into a spectrum lease with FirstNet prior to gaining authority to deploy and operate the state RAN utilizing the spectrum licensed to FirstNet. Thereafter, states will also be required to comply with FirstNet, and as applicable, the Contractor's network policies.

In the event that a particular state or territory notifies FirstNet that it intends to exercise this right, the Contractor's total proposed payments to FirstNet will be accordingly adjusted downward (if positive values of the payments were proposed for that state/territory) or upward (if negative values of the payments were proposed for that state/territory). For example, if an Offeror had proposed a $10 payment for State X, and State X notifies FirstNet that it intends to take responsibility for the deployment and operation of the RAN in its state, the Offeror's payments to FirstNet will be reduced by $10.

In accordance with Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.3.1, General and Structural Requirements, Offerors shall submit option pricing for state RAN deployment and operation for each of the 56 states and territories that occurs after an initial state decision to assume its own RAN deployment and operation. The option pricing should reflect the Offeror's consideration that the decision was delayed and that pricing needs to be valid for a longer period of time.

B.2 Pricing Schedules and Task Orders

The Offeror is to respond to the instructions contained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, for the IDIQ contract as well as any pricing instructions. For the IDIQ contract, the Offeror shall provide pricing for the life of the contract. Pursuant to Section L, Instructions, Conditions, and Notices to Offerors or Respondents, the Offeror shall propose pricing for each of the Day 1 task orders as specified in Section F, Deliverables and Performance, Section F.2, Term of the Contract and Task Orders. The Offeror shall utilize the pricing templates within Section J, Attachment J-13, Pricing Template, to submit pricing with their proposal. For proposal preparation and evaluation purposes, the Pricing Template includes the following dates:

- Estimated award date for the IDIQ contract and Day 1 task orders – November 1, 2016
- Estimated task order date for Initial FirstNet-Deployed RAN States – April 30, 2017
- Estimated task order date for Delayed FirstNet-deployed RANs – Up to and including June 19, 2019

These estimated dates may vary and the Offeror shall be expected to adhere to the price validation periods stated in Section A, Solicitation, Offer, and Award, and as stated herein.

B.2.1 Day 1 Task Orders

The Government anticipates the Day 1 task orders issued as a result of this RFP will be Performance-Based-Service-type orders. Pricing should be provided for each of the Day 1 task orders identified below and submitted in accordance with the instructions contained in Section L, Instructions, Conditions, and

Notices to Offerors or Respondents, and as reflected in the Pricing Template (Section J, Attachment J-13).

1. Delivery Mechanism for State Plans
2. State Plan Development and Refinement
3. NPSBN Functions

The CLINs that are related to payments to the Contractor shall be consistent with the Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

B.2.1.1 Task Order 1 – Delivery Mechanism for State Plans

Under this task order, the Contractor shall develop a Web-based mechanism for delivering state plans that will allow FirstNet to publicly house its RAN deployment and operations plans for each of the 56 states and territories. Proposed payments to the Contractor associated with this task order should be included in the Section J, Attachment J-13, Pricing Template, Payments to Contractor tab. The objectives regarding the delivery mechanism for state plans are contained in Section J, Attachment J-18.

B.2.1.2 Task Order 2 – State Plan Development and Refinement

Under this task order, the Contractor shall provide support to FirstNet in its development and refinement of state plans for the deployment and operation of RANs in each of the 56 states and territories. Proposed payments to the Contractor associated with this task order should be included in Section J, Attachment J-13, Pricing Template, Payments to Contractor tab.

B.2.1.3 Task Order 3 – NPSBN Functions

The Contractor shall deploy, operate, and maintain the nationwide Core under this task order. Details regarding the Core design and operation are to be provided as noted in Section F, Deliverables and Performance, Section F.4.2.22, Core Network Design. Also, this task order encompasses activities described in the Products and Architecture and Business Management milestones detailed in Section J, Attachment J-8, IOC/FOC Target Timeline, for the entire period of performance (see Section F, Deliverables and Performance, Section F.2.1.3, NPSBN Functions). Disbursement of payments to the Contractor will be contingent upon acceptance, in accordance with and applicable to all IOC/FOC milestones. Proposed payments to the Contractor associated with this task order should be included in the Section J, Attachment J-13, Pricing Template, Payments to Contractor tab.

B.2.2 State and Territory Task Order(s) – Initial FirstNet-Deployed RAN States

The Offeror's proposed solution and pricing approach shall include separable submissions for delivery of the NPSBN for each of the 56 states and territories that select a FirstNet-deployed RAN, pursuant to instructions contained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, and the Pricing Template (Section J, Attachment J-13). These submissions should encompass pricing as identified in Section L.3.3.3, Payments to FirstNet. The Government may issue these task orders within 120 calendar days of state plan delivery at the levels proposed by the Offeror. The Government reserves the right to issue a subsequent task order for each state or territory individually or a combination thereof. Under these task orders, the Contractor shall be required to make payments to FirstNet based on the aggregate of the positive and/or negative values (as identified in Section L,

Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.3.3, Payments to FirstNet) associated with each state and territory.

B.2.3 State and Territory Task Order(s) – Delayed FirstNet-Deployed RANs

The Offeror's proposed solution and pricing approach shall include separable submissions, pursuant to instructions contained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, for delivery of the NPSBN for each of the 56 states and territories that will rely on FirstNet to deploy and operate the RAN. This pricing approach applies to states and territories that initially notified FirstNet of their intent to deploy and operate a state-deployed RAN, but do not fulfill their statutory obligations per the Act. The Government may issue these task orders within 900 calendar days of state plan delivery at the levels proposed by the Offeror. These submissions should encompass pricing as identified in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.3.4, Delayed Payments to FirstNet. The Government reserves the right to issue a subsequent task order for each such state or territory individually or a combination thereof. Under these task orders, the Contractor shall be required to make payments to FirstNet based on the aggregate of the positive and/or negative values (as identified in Section L.3.3.4, Delayed Payments to FirstNet, and Section J, Attachment J-13, Pricing Template) associated with each state and territory.

B.2.4 Other Task Orders

The Government reserves the right to issue subsequent task orders that are considered within the scope of the contract. For example, a subsequent task order or modified task order may be issued in the event that a state or territory is successful in assuming responsibility for deploying and operating its own RAN. In this scenario, the Government may make available applicable integration and Core operating fees, as negotiated between the Government and the Contractor, as authorized in the Act, and as executed in a subsequent task order award or modification.

B.3 North American Industry Classification System Code

The following North American Industry Classification System (NAICS) code is the primary NAICS code applicable to this acquisition:

517210 Wireless Telecommunications Carriers, business size standard of 1,500 employees

B.4 Financial Resources and Capabilities

The deployment, ongoing operations, and recapitalization of the NPSBN will require significant financial resources and capabilities. The $6.5 billion budget authority—discussed further in Section B.4.1, Budget Authority, below—represents the maximum funding available that may be reduced depending on the number of states and territories that successfully deploy, operate, and maintain their own RAN.

FirstNet has several types of financial resources available, which are defined below.

B.4.1 Budget Authority

Under provisions in the Act, FirstNet was provided an initial $7 billion in budget authority. For proposal preparation purposes, the Offeror should assume FirstNet is contributing up to $6.5 billion of allocated

funding to the NPSBN obligated via the Day 1 and subsequent task orders. Funding contributions from FirstNet will only be payable upon acceptance of the IOC/FOC milestones (as described in Section J, Attachment J-8, IOC/FOC Target Timeline), as they correlate to the proposed solution.

B.4.2 Public Safety Revenue

FirstNet expects that the Contractor may charge fees associated with using the NPSBN to public safety end users. The Contractor will retain this revenue.

B.4.3 Excess Network Capacity

FirstNet is authorized under the Act to realize the value associated with the lease of network capacity that is unused by Public Safety Entities—i.e., excess network capacity—through the terms and conditions of this contract as defined in the Act (Covered Leasing Agreement) and interpreted in FirstNet's public notices. As part of the pricing objective, and in addition to retaining revenue from public safety users using the NPSBN, the Contractor will also have access to, and the ability to derive revenue from, all excess network capacity from FirstNet-deployed RANs. This results in the ability of the Contractor to utilize all 20 MHz of Band 14 spectrum under FirstNet's license in order to derive revenue that may be retained by the Contractor. Should a state or territory successfully assume responsibility for deploying and operating its own RAN, the Contractor may not receive access to the network capacity value for that state or territory through this contract.

B.4.4 FirstNet Operational Sustainability

FirstNet must be sustainable on an ongoing basis and in any given Government fiscal year (FY) pursuant to the Act and other applicable statutes. To achieve this, the Offeror shall propose payments to FirstNet as described in Section B.2.2, State and Territory Task Order(s) – Initial FirstNet-Deployed RAN States, and Section B.2.3, State and Territory Task Order(s) – Delayed FirstNet-Deployed RANs, that are equal to, or in excess of, minimum payments for FirstNet's operational sustainability. The Offeror should assume the minimum payment threshold (Table 1 FirstNet Minimum Payment Thresholds) and actual payments will be adjusted up to 900 days when completing the Delayed Payments to FirstNet portion of the Pricing Template (Section J, Attachment J-13). Payments to FirstNet will begin when FirstNet awards the state and territory Delayed FirstNet-Deployed RANs subsequent task order(s).

The FirstNet minimum payments—detailed in Table 1 FirstNet Minimum Payment Thresholds below—represent estimated costs that FirstNet expects it may incur over the life of the contract. This estimate includes base operating and general administrative costs, including required personnel associated with the currently contemplated Operational Architecture as set forth in Section J, Attachment J-7, as well as costs for establishing a network re-investment reserve fund, supporting recapitalization of the network, acquisition support and planning, and other authorized purposes under the Act and applicable laws. FirstNet has phased the yearly profile of the FirstNet minimum payment thresholds taking into account the Contractor's anticipated ramp-up in the deployment and operations of the NPSBN to help ensure the minimum necessary to maintain initial FirstNet sustainability in accordance with current operating assumptions, while also reducing the financial burden on the Contractor during initial deployment of the network. Any revenue FirstNet generates from the required payments hereunder will be reinvested into the construction, maintenance, operation, or other improvements to the network per Section 6208 of the Act. The Offeror shall propose these payments in accordance with the

instructions provided in Section L, Instructions, Conditions, and Notices to Offerors or Respondents. The Offeror may propose payments above these minimum payment thresholds.

Table 1 FirstNet Minimum Payment Thresholds

Contract Year	Payment
1	$80,000,000
2	$80,000,000
3	$80,000,000
4	$80,000,000
5	$80,000,000
6	$130,000,000
7	$130,000,000
8	$130,000,000
9	$130,000,000
10	$130,000,000
11	$205,000,000
12	$205,000,000
13	$205,000,000
14	$205,000,000
15	$205,000,000
16	$305,000,000
17	$305,000,000
18	$305,000,000
19	$305,000,000
20	$305,000,000
21	$305,000,000
22	$430,000,000
23	$430,000,000
24	$430,000,000
25	$430,000,000

B.4.5 Adjustment to Proposed Payments to the Contractor for State RAN Provision

Pursuant to Section 6302 of the Act, states and territories may choose to undertake the responsibility for deploying, operating, and maintaining the RAN within the state or territory. In addition, NTIA is authorized to administer a RAN construction grant program for states and territories if any state or territory assumes responsibility for its own RAN deployment and operation and applies for a grant. In the event that a state or territory elects to pursue responsibility for deploying and operating its own RAN, the payments from FirstNet to the Contractor, as proposed by the Offeror in the relevant pricing worksheets (see Section J, Attachment J-13, Pricing Template), will be adjusted downward for each state or territory that notifies FirstNet that it intends to deploy its own RAN. For example, if an Offeror had proposed a $10 payment to the Contractor for State 2, and State 2 notifies FirstNet that it intends to take responsibility for the deployment and operation of the RAN in its state, FirstNet's payments to the contractor will be reduced by $10.

The amount of funding between FirstNet and the NTIA grant program authorized in Section 6302 of the Act for those states or territories that take on RAN responsibility will be determined after award. The portion of the funding ultimately determined to be necessary for the grant program under Section 6302

will be deducted from the overall amount of cash available to the Contractor and may be informed by the Offeror's proposal as detailed in the Payments to Contractor worksheet in the Pricing Template (Section J, Attachment J-13). NTIA has informed FirstNet that it intends to review several factors as part of its potential grant program, which may include cost and value information compared to the FirstNet state plans, and final grant funding in any given state or territory may be lower than RAN-related build costs as proposed by the Offeror.

B.5 Other Task Order Costs

Other costs associated with subsequent task orders, not identified herein, shall be task-order-dependent. The price(s) charged to the Government for such item(s) or service(s) shall be procured in accordance with all required laws and regulations. The Contractor shall seek competitive bids or use other means to support price reasonability for all lots of equipment, supplies, and/or services exceeding the micro-purchase threshold, as identified in the FAR 2.1, Definitions, which are acquired under this contract.

B.6 Contract Minimum and Maximum Thresholds

During the life of this contract, the Government is not obligated to purchase services above the guaranteed minimum for the entire period of performance for this IDIQ, which is $150 million.

The contract ceiling for the entire period of performance for this IDIQ is $100 billion.

Table of Contents

C Statement of Objectives

The First Responder Network Authority (FirstNet) Nationwide Public Safety Broadband Network (NPSBN) Statement of Objectives (SOO) defines the objectives for the NPSBN as shown herein. FirstNet has adopted an objectives-based approach in this Request for Proposal (RFP), rather than a traditional requirements-driven model, to provide industry the maximum opportunity and flexibility in the development of innovative solutions for the NPSBN. Providing this flexibility enables Offerors to illustrate their intent in their proposals to meet or exceed the high-level objectives outlined below. These objectives establish high-level outcomes and should assist the Offerors in their establishment of the Performance Work Statement, as outlined in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.1.1, Section One – General.

C.1 Background

In February 2012, Congress enacted the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), containing provisions to create an interoperable NPSBN for Public Safety Entities (PSEs). A PSE is defined in Section 6001(26) of the Act as an "entity that provides public safety services" 47.U.S.C. § 1401(26). The Act created FirstNet, an independent authority within the National Telecommunications and Information Administration, and outlined a governing framework for the deployment and operation of the NPSBN based on a single nationwide network architecture.

C.2 Requirements Derivation

The Act required the establishment of a Board to govern the activities of FirstNet. In turn, the FirstNet Board authorized its management team, including a program office, to carry out the operations of the organization, including the development of the SOO contained herein.

In addition, the Act established within the Federal Communications Commission (FCC) an advisory board to create minimum interoperability requirements for the NPSBN. The Technical Advisory Board (TAB) for First Responder Interoperability issued these requirements in 2012 in a report entitled, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network* (FCC TAB RMTR) (Section J, Attachment J-3). References to the FCC TAB RMTR throughout this document refer to the original report adopted on June 21, 2012, by the FCC and the associated clarification issued by the TAB and received by the FCC on June 6, 2012. This is also referenced in the FCC's transmittal on June 21, 2012. Subsequently, the FirstNet Program Management Office (PMO) initiated requirements analysis and acquisition planning. Through this process, it was determined that provisions in the Act necessitated the establishment of a minimum set of requirements for the NPSBN. The PMO also adopted an enterprise architecture approach that identified the need for additional requirements to support an enterprise services capability.

This SOO lists high-level objectives with minimum requirements, allowing latitude for Offerors to define implementation details. This comprehensive, yet flexible approach allows Offerors to be highly innovative in proposing solutions that ensure nationwide interoperability.

C.3 Program Description

FirstNet is seeking a comprehensive network solution covering each of the 56 states and territories. The comprehensive network solution shall provide FirstNet services that include: the deployment and provisioning of a nationwide Core Network ("Core"), and Radio Access Network (RAN) services;

backhaul, aggregation, and the use of national transport networks and operation centers; a device ecosystem; use of network infrastructure; deployable capabilities; use of operational and business support systems; an applications ecosystem; network services; and the integration, maintenance, operational services, and ongoing evolution of these systems required to function fully as an operational wireless 3rd Generation Partnership Project (3GPP) standards-based Long Term Evolution (LTE) NPSBN.

Spectrum Act section 6202(b)(2) indicates that the NPSBN RAN comprises "cell site equipment, antennas, and backhaul … that are required to enable wireless communications with devices." The RAN utilizes Band 14 radio spectrum.

FirstNet intends to maximize the NPSBN's value to public safety while meeting its financial sustainability obligations under the Act. Therefore, solutions may include, for example, but are not limited to (1) "in kind" and/or monetary value provided by the Contractor in consideration of secondary use of FirstNet's excess network capacity and (2) various partnerships and business arrangements that monetize new public safety market offerings via devices, applications, and other value-added benefits and services that enhance the public safety user experience.

This acquisition considers the value provided for leadership, program management, public safety adoption, customer care, life-cycle management, financial sustainability, coverage, capacity, network architecture, and a product plan, among many other factors. FirstNet does not seek to dictate the deployment strategy of the Offeror or the manner in which parties may or may not seek to align themselves through partnerships, joint ventures, or other vehicles to produce an offer in response to this solicitation. Rather, FirstNet seeks to outline broad objectives that must be accomplished by the Offeror and encourages innovative solutions that will meet and exceed the needs of both FirstNet and public safety. This acquisition is not limited by any particular solution nor to any specific type or character of Offeror, but rather is open to all entities, whether traditional wireless incumbents or new entrants, provided FirstNet's objectives and minimum requirements are satisfied.

FirstNet must create the NPSBN within the financial parameters outlined in the Act and ensure its financial sustainability through federal funding, user fees, and agreements with the Contractor that will leverage the value of excess network capacity. In addition, FirstNet must provide services at competitive prices given constrained local, state, and federal budgets. In undertaking this task, FirstNet must leverage—to the extent economically desirable—existing infrastructure, obtain optimal value for excess network capacity, and optimize its pricing structure so that FirstNet can deliver a high-quality, affordable broadband network and services to the nation's PSEs.

Section 6201 of the Act required the FCC to reallocate and grant a license to FirstNet for the use of the 700 MHz D block spectrum and existing public safety broadband spectrum. FirstNet will make available to the Contractor all 20 MHz of the Band 14 spectrum to be used for NSPBN purposes and enter into Band 14 Covered Leasing Agreements (CLAs). The Public Land Mobile Network (PLMN) ID for the NPSBN will be provided by FirstNet. Under a CLA, as contemplated by Section 6208(a)(2) of the Act, the Contractor can monetize all 20 MHz of the spectrum both for primary use by PSEs and secondary use. FirstNet's 20 MHz of the 700 MHz spectrum offers several unique characteristics including 1) unencumbered nationwide access and use that is not limited to a defined geographical area; 2) Part 90 service rules governing the spectrum, which enables the use of higher powered devices that can improve coverage; and 3) spectrum that does not count against the sub 1 GHz spectrum screen restrictions for wireless carriers, enabling Offerors to bid on other spectrum. These unique characteristics provide the Contractor a valuable finite resource that is not available in any other highly coveted low-band spectrum.

FirstNet will bring to PSEs an interoperable NPSBN with quality of service, priority usage, and preemption. In addition, the NPSBN will be hardened, as needed, from the physical perspective and will be resilient, secure, and highly reliable from the network perspective. Furthermore, the NPSBN will provide to public safety agencies both national and local control over prioritization, preemption, provisioning, and reporting.

The NPSBN and associated devices will be branded as FirstNet, consistent with applicable laws and regulations. While FirstNet will maintain oversight responsibilities for all functions, as outlined in Section J, Attachment J-7, Operational Architecture, it is expected that the Contractor will be responsible for executing marketing, product management; sales; distribution; customer care; communications; strategic partnering; and network deployment, operation, and evolution.

C.4 Scope

Public safety requires a nationwide interoperable broadband network that covers urban, suburban, and rural areas and meets the information and communications technology needs associated with public safety's mission. This acquisition of services includes business, technical, financial, operational, logistical, and program management components. FirstNet requires continuous upgrade and innovation of the NPSBN throughout the life of the contract as LTE and wireless broadband technologies (e.g., 5G, 6G) evolve, as public safety needs expand, and as new capabilities and technologies become accepted and available.

The NPSBN service, and therefore the Contractor's operational management of the NPSBN, shall support the operational needs of public safety, ranging from routine law enforcement, fire, rescue, emergency response, and similar operations through major natural and man-made disasters and homeland security and homeland defense missions.

C.5 Objectives

It should be noted that the objectives for the NPSBN are from the government's perspective and, as such, are nationwide in scope. These objectives ensure that the NPSBN operates as a nationwide interoperable network, guaranteeing seamless interoperability for each of the 56 states and territories.

The FirstNet objectives for NPSBN services follow:

1) **BUILDING, DEPLOYMENT, OPERATION, AND MAINTENANCE OF THE NPSBN:** Provide nationwide interoperable public safety broadband network service that ensures network coverage 24 hours a day, 7 days a week, 365 days a year and complies with the technical requirements referenced herein, throughout the RFP and its attachments.

2) **FINANCIAL SUSTAINABILITY:** Maximize the impact of government funding and leverage all 20 MHz of Band 14 to build, deploy, operate, and maintain the NPSBN to serve public safety and for secondary use while ensuring a self-sustaining business model including making payments to FirstNet as identified in Section B, Supplies or Services and Prices/Costs.

3) **FIRST RESPONDER USER ADOPTION:** Establish (i) compelling, differentiated, and competitively priced service packages and (ii) sales, distribution, and marketing capabilities to ensure adoption of FirstNet products and services by a majority of eligible PSEs within four years of award (refer to Initial Operational Capability [IOC]-5 in Section J, Attachment J-8, IOC/FOC Target Timeline). NPSBN

services, at a minimum, shall include data, voice services, messaging, machine-to-machine, virtual private network (VPN), video, unique public safety mission-critical services, and location services.

4) **DEVICE ECOSYSTEM:** Provide and maintain a 3GPP-compliant, Band-14-capable device portfolio that evolves with the 3GPP standards and provides functionality and price points that meet the needs of the FirstNet public safety customer base and drive substantial subscribership. FirstNet anticipates NPSBN public safety customers will expect mass market as well as ruggedized devices that are capable of gloved, one-handed, or hands-free operation as well as those capable of multimedia and high-definition data transmission both from humans and machine-based sensors. The ecosystem shall support Bring Your Own Device (BYOD) as well as, at a minimum, devices that:

- Operate seamlessly on the NPSBN and roam onto networks, including non-Band 14 commercially available networks
- Interoperate with FirstNet's applications ecosystem
- Support associated Universal Integrated Circuit Card (UICC) features and options, including the ability to home and, if applicable, roam on to multiple networks while prioritizing them appropriately
- Support secure containers to isolate FirstNet applications
- Operate seamlessly with a comprehensive device management system to allow remote provisioning and control

5) **APPLICATIONS ECOSYSTEM:** Provide an applications ecosystem that supports the NPSBN with capabilities and services relevant to public safety. The ecosystem shall include, at a minimum:

- An evolving portfolio of mobile and enterprise applications, as well as cloud services
- An applications development platform
- A vibrant third-party applications developer community
- An applications store
- Local control of users, subscriptions, services, and applications
- User friendly federation of identity management
- Data, application, and resource sharing across diverse PSEs
- Core service and application delivery platforms
- Data and applications security and privacy compliance across local, tribal, state, regional, and federal users (additional information in objective 9 below and Section J, Attachment J-10, Cybersecurity)

6) **ACCELERATED SPEED TO MARKET:** Achieve operational capabilities in accordance with the schedule and feature sets denoted in Section J, Attachment J-8, IOC/FOC Target Timeline, which may include an initial provision for operating the NPSBN using existing wireless services (similar to that of a mobile virtual network operator [MVNO]), Band 14 capabilities, significant subscribership to the NPSBN, and substantial rural coverage milestones in accordance with the IOC/FOC milestones.

7) **USER SERVICE AVAILABILITY:** Provide a broadband service with availability of 99.99%, exclusive of planned maintenance windows, as measured in a rolling 12-month window within each reporting area. Offerors should consider areas that contain mission-critical infrastructure as needing enhanced hardening and increased availability. Service restoration activities shall be undertaken with the highest available priority but shall not exceed two hours for any impaired service. For restoration of service via temporary or secondary service capabilities, the temporary or secondary service must be transparent to the users and provide similar capability.

8) **SERVICE CAPACITY:** Provide service capacity to support geographically dispersed public safety usage (in accordance with FCC TAB RMTR 4.4.6.5, Capacity) throughout the life of the contract. Section J, Attachment J-1, Coverage and Capacity Definitions, includes a map noting first responder density and current mobile data usage. This will serve as a baseline for public safety data demand, and mobile data demand is expected to increase throughout the life of the contract.

9) **CYBERSECURITY:** Provide cybersecurity solutions using the extensive set of industry standards and best practices contained in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) security guidance for networks (ISO/IEC 27033, ISO/IEC 17099, and ISO/IEC 27002), FCC TAB RMTR, and 3GPP specifications (TS23.401, TS33.102, TS33.210, TS33.310, TS33.401, and TS33.402). Provide encryption capabilities to support federal, state, and local public safety users. Protective measures will need to be applied end to end across the FirstNet enterprise environment and will include securing user equipment (UE), applications running on UE, the RAN, and the Core network. Additionally, considerations to support Identity, Credential, and Access Management in a user friendly, secure, federated fashion will be key to any successful cybersecurity solution (details can be found in Section J, Attachment J-10, Cybersecurity).

10) **PRIORITY SERVICES:** Provide a solution that allows the assignment of quality of service, priority, and preemption (QPP) parameters to user profiles using the standard service control parameters defined by 3GPP and the Internet Engineering Task Force, including Access Class, Quality Class Indicator (QCI), Allocation and Retention Priority (ARP), and Differentiated Service (Diff Serve). Allow control and management of static and dynamic assigned QPP parameters for public safety users and the ability to change user profiles in real time in response to incidents. User profile assignments and changes should be managed locally by PSEs.

11) **INTEGRATION OF STATE-DEPLOYED RANs**: Integrate the NPSBN across state and territory deployed RANs so that users operate without service interruptions, including when crossing RAN service area boundaries. Additional details are provided in Section J, Attachment J-4, System and Standards Views.

12) **INTEGRATION OF EXISTING COMMERCIAL/FEDERAL/STATE/TRIBAL/LOCAL INFRASTRUCTURE TO SUPPORT NPSBN SERVICES:** Integrate existing assets— where economically desirable in accordance with Section 6206 of the Act and as further interpreted in FirstNet's request for public comments — with an emphasis on assets owned and operated by rural telecommunications providers.

13) **LIFE-CYCLE INNOVATION:** Evolve the NPSBN solution—including products and services—and incorporate 3GPP LTE standards as they evolve and mature throughout the life of the contract, in accordance with the FCC TAB RMTR, the Act, including in particular Section 6206(c)(4), and the attachments in Section J.

14) **PROGRAM AND BUSINESS MANAGEMENT:** Provide program management for the NPSBN in accordance with the Project Management Institute or other applicable industry standards, Information Technology Infrastructure Library (ITIL®) or equivalent, and Government Accountability Office cost guidelines.

15) **CUSTOMER CARE AND MARKETING:** Market NPSBN products and services to public safety users in all states, territories, and tribal lands. Provide highly responsive and quality customer acquisition, service, and customer care. Support development and refinement of state plans, in consultation with FirstNet, and an online tool for their delivery. Provide life-cycle service and support to all users.

16) **FACILITATION OF FIRSTNET'S COMPLIANCE WITH THE ACT AND OTHER LAWS**: Perform all objectives and provide information and services in a manner that facilitates FirstNet's compliance with its statutory requirements under the Act and all other applicable laws.

C.6 State Coverage Objectives

The Act (Section 6206(b)(3)) requires a phased deployment of the NPSBN with substantial rural coverage milestones as part of each phase. Deployment phases and substantial rural coverage milestones are outlined in Section J, Attachment J-8, IOC/FOC Target Timeline. The state NPSBN coverage objectives are contained in image file (.png) format (Section J, Attachment J-1, Coverage and Capacity Definitions).

FirstNet is required to submit a state plan to each of the 56 states and territories. The Contractor will not be required to meet coverage objectives for state-deployed RANs. States deploying their own RANs will be required to comply with Section J, Attachment J-4, System and Standards Views, and applicable Spectrum Manager Lease Agreement(s).

C.7 Minimum Technical Requirements

The Act (Section 6203(c)) required the FCC TAB to develop the minimum technical requirements for the NPSBN. On June 21, 2012, the FCC approved by Order (FCC 12-68) the FCC TAB RMTR report. The Offeror's solution shall comply with these minimum requirements (Section J, Attachment J-3, FCC TAB RMTR), including the clarification issued by the TAB on June 6, 2012 (also referenced in the FCC's 12-68 order).

The Act requires FirstNet to comply with 3GPP LTE standards and open, non-proprietary, commercially available standards. Contractor-provided NPSBN services shall comply with Section J, Attachment J-4, System and Standards Views.

C.8 Performance Standards

The Offeror shall propose service functions consistent with FirstNet's objectives, and propose necessary performance standards, metrics, and deliverables as defined in Section J, Attachment J-6, Quality Assurance Surveillance Plan, and Section F, Deliverables and Performance.

C.9 Delivery Schedule

The Contractor shall consider the target milestone delivery schedule as outlined in Section J, Attachment J-8, IOC/FOC Target Timeline. This milestone delivery schedule is consistent with the current 3GPP release schedule. Beyond FOC, the Contractor and FirstNet require an ongoing roadmap and product management process that allows for joint agreement on features, timing, and pricing.

Table of Contents

D Packaging and Marking

D.1 FAR 52.252-1 – Solicitation Provisions Incorporated by Reference (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The Offeror is cautioned that the listed provisions may include blocks that must be completed by the Offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the Offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at these addresses:

- Federal Acquisition Regulation (FAR) Clauses: https://www.acquisition.gov/?q=browsefar
- Department of Commerce Acquisition Regulation (CAR) Clauses: http://farsite.hill.af.mil/vfcara.htm
- Department of the Interior Acquisition Regulation (DIAR) Clauses: http://farsite.hill.af.mil/vfdiara.htm

D.2 Packaging and Marking

All items provided under this contract shall be packaged and marked in accordance with industry best practices.

Table of Contents

E Inspection and Acceptance

The terms and conditions described herein for the First Responder Network Authority (FirstNet) Nationwide Public Safety Broadband Network (NPSBN) Indefinite Quality/Indefinite Quantity (IDIQ) contract shall apply to each task order. The Contracting Officer's Representative (COR) and/or any inspectors designated by the Contracting Officer will inspect and determine final acceptance of the supplies/services provided hereunder. The places of inspection for deliverables required under this contract shall be at the addresses for deliverables set forth in Section F, Deliverables and Performance, or as directed by the COR. Section G, Contract Administration Data, of the resultant contract and any task order will identify the COR and/or any inspectors designated by the Contracting Officer.

E.1 General Acceptance Criteria

General quality measures, as set forth below, apply to each work product received from the Contractor. The COR or designated inspector will review each work product against these measures before determining acceptance.

- **Accuracy** – Work products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- **Clarity** – Work products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
- **Consistency to Requirements** – All work products shall satisfy the requirements of this contract.
- **File Editing** – All text and diagrammatic files shall be editable by the Government.
- **Format** – Work products shall be submitted in hard copy (where applicable) and in media, unless otherwise specified herein. Hard-copy formats shall follow any specified directives or manuals. Media formats shall follow the mutual agreement of the parties unless specified elsewhere.
- **Timeliness** – Work products shall be submitted on or before the due date specified herein or submitted in accordance with a later scheduled date determined by the Government.

E.2 Quality Assurance

The COR and/or designated inspector will review, for completeness, preliminary or draft documentation that the Contractor submits and may return it to the Contractor for correction. The absence of any comments by the COR and/or inspector shall not relieve the Contractor of the responsibility for complying with the requirements of this work statement. Final approval and acceptance of documentation required herein will be by letter of approval and acceptance by the COR or inspector. The Contractor shall not construe any letter of acknowledgment of material receipt as a waiver of review or as an acknowledgment that the material is in conformance with this work statement. Any approval given during preparation of the documentation or approval for shipment will not guarantee the final acceptance of the completed documentation.

E.3 Department of Commerce Acquisition Regulation

The contract clauses set forth in the following paragraphs of the CAR—as designated in Table 1 CAR Clauses Incorporated—are incorporated in this contract with the same force and effect as though set forth herein in full text. The designated clauses are incorporated as they appear in the CAR on the date of this contract, notwithstanding the date referenced.

Table 1 CAR Clauses Incorporated by Reference

Clause	Title	Date
1352.246-70	Place of Acceptance	APR 2010

E.4 52.252-2 Clauses Incorporated by Reference (FEB 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

- FAR Clauses: http://www.acquisition.gov/comp/far/loadmainre.html
- CAR Clauses: http://farsite.hill.af.mil/vfcara.htm
- DIAR Clauses: http://farsite.hill.af.mil/vfdiara.htm

(End of Clause)

Table 2 FAR Clauses Incorporated by Reference

Clause	Title	Date
52.246-2	Inspection of Supplies – Fixed Price	AUG 1996
52.246-4	Inspection of Services – Fixed Price	AUG 1996
52.246-6	Inspection of Time-and-Material and Labor-Hour	MAY 2001
52.246-16	Responsibility for Supplies	APR 1984

Table of Contents

List of Tables

F Deliverables and Performance

F.1 FAR 52.252-2 Clauses Incorporated by Reference (FEB 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

- Federal Acquisition Regulation (FAR) Clauses: https://www.acquisition.gov/?q=browsefar
- Department of Commerce Acquisition Regulation (CAR) Clauses: http://farsite.hill.af.mil/vfcara.htm
- Department of the Interior Acquisition Regulation (DIAR) Clauses: http://farsite.hill.af.mil/vfdiara.htm

(End of Clause)

Table 1 Federal Acquisition Regulation Clauses Incorporated by Reference

Clause	Title	Date
52.242-15	Stop-Work Order	AUG 1989
52.242-17	Government Delay of Work	APR 1984
52.247-34	F.O.B Destination	NOV 1991

F.2 Term of the Contract and Task Orders

The term of this Indefinite Delivery, Indefinite Quantity (IDIQ) contract will be for a period of 25 years beginning on the date of award, currently anticipated on November 1, 2016.

The term of any subsequent task order issued under this IDIQ contract will specify the period of performance applicable to that task order.

F.2.1 Day 1 Task Order Period of Performance

F.2.1.1 Delivery Mechanism for State Plans

The delivery mechanism for state plans task order period of performance is from the date of award through three years post award. This is based on commencement of performance on November 1, 2016; anticipated delivery date of the delivery mechanism on or before February 1, 2017, allowing the remaining period of performance for use and/or enhancements of the mechanism, if needed, (February 2, 2017 through November 1, 2019).

F.2.1.2 State Plan Development and Refinement

The state plan development and refinement task order period of performance is from the date of award through one year post award. This is based on commencement of performance on November 1, 2016; anticipated delivery date of the delivery mechanism on or before February 1, 2017, allowing the remaining period of performance for support, coordination and refinement of state plans, as needed, (February 2, 2017 through November 1, 2017).

F.2.1.3 NPSBN Functions

The NPSBN functions task order period of performance is from the date of award through November 2041. However, it may be subject to license renewal and reauthorization.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

F.3 Place of Performance

Services may be provided off-site, on-site, or through a combination of the two, depending on program requirements specified herein or in individual task orders. However, the First Responder Network Authority (FirstNet) anticipates the majority of the work will be performed at the Contractor's facilities unless otherwise stated.

F.4 Meetings, Reports, and Other Deliverables

Instructions for Contractor-proposed deliverables and FirstNet-required deliverables are noted below and in Section L, Instructions, Conditions, and Notices to Offerors or Respondents. All deliverables shall be submitted to the Contracting Officer's Representative (COR) or posted in a format specified by the Contractor for online access by the Contracting Officer (CO) and other government personnel designated by the CO. The CO will provide the Contractor with the names and addresses of any additional distribution and/or online access for these deliverables. Except as indicated herein, or with explicit written permission from FirstNet, deliverables shall not contain proprietary or copyrighted information or have any restriction on reproduction and/or distribution.

Unless otherwise specified, the Government will have approximately 15 working days to review the deliverable and provide comments back to the Contractor. If the deliverable is acceptable, the COR will notify the Contractor; otherwise, comments will be provided for revision/rework. The Contractor will have 10 working days from receipt of comments to incorporate changes and submit the final deliverable to the Government. Deliverables are not considered accepted by the Government until the COR or CO provides specific notification to the Contractor (see Section E, Inspection and Acceptance, Section E.2, Quality Assurance).

All days identified in the Deliverables Table are workdays unless otherwise specified. All deliverables shall be in a Contractor-recommended format and must be approved by the COR. The Contractor shall use Microsoft Office products and Adobe PDF format to prepare any deliverable that is to be submitted electronically.

F.4.1 Proposed Deliverables

In support of this Request for Proposal (RFP), Section L, Instructions, Conditions and Notices to Offerors or Respondents, Section L.3.1.8, Section Eight – Deliverables Table, instructs the Offeror to provide a Deliverables Table that defines what deliverables the Contractor will provide following the contract award. The Deliverables Table shall match the format and structure provided in Section J, Attachment J-16, Deliverables Table, and shall be incorporated into this contract at award.

F.4.2 FirstNet-Required Deliverables

The following descriptions provide details about each deliverable, including the purpose, format, and frequency.

F.4.2.1 Deployment Plan ("State Plan") for States and Territories

In accordance with the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), FirstNet must present a plan to the governor of each state and territory that includes, among other things, "… details of the proposed plan for buildout of the nationwide interoperable, broadband network in such State …"

In support of this requirement, the Contractor shall deliver a detailed plan, for each of the 56 states and territories, noting the details of the proposed plan for buildout of the Nationwide Public Safety

Broadband Network (NPSBN) in such state or territory. The plan must include elements that are required of FirstNet by the Act, elements states and territories will need for the governor's decision, and elements that the Federal Communications Commission will require to assess state-deployed Radio Access Networks (RANs).

The plan for each state and territory shall be delivered using the Web-based delivery tool outlined in Section J, Attachment J-18, Delivery Mechanism Objectives for State Plans, according to the proposed Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones established in Section J, Attachment J-8, IOC/FOC Target Timeline.

Delivery date for these deliverables is to be proposed by the Offeror.

F.4.2.2 Coverage and Capacity

The Contractor shall provide the following coverage and capacity deliverables post contract award. If the Offeror's solution includes non-Band 14 RAN, include the non-Band 14 coverage maps and associated network statistics, as noted below.

F.4.2.2.1 Coverage, Population, and Capacity Maps

Within 30 days of contract award, the Contractor shall submit an updated package of coverage, population, and capacity maps and network statistics—as defined in Table 2 Coverage Maps and Table 3 Network Statistics for each of the 56 states and territories. The Contractor shall also update the proposed Coverage and Capacity Template provided in Section J, Attachment J-17, including completion of the "Site Summary Tab," noting site locations nationwide. The Contractor shall note changes that have occurred subsequent to the proposal submission in the updated package and Coverage and Capacity Template.

Table 2 Coverage Maps

Level	Band	Phase	Number of Maps Required	Format	Submittal Method
Nationwide	Non-Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC	Six (6) maps of each file type, depicting coverage by technology: Long Term Evolution (LTE), 3G, 2G, and roaming.	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files	Files should be provided via Secure File Transfer (SFT) with Offeror-provided credentials or Offeror-provided portable drive
Nationwide	Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC	Six (6) maps of each file type with the LTE analysis layers specified above	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files	Files should be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive

Table 3 Network Statistics

Coverage Type	Level	Phase
Non-Band 14 Area Covered **	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Non-Band 14 Population Covered **	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Band 14 Area Covered	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Band 14 Population Covered	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Band 14 Network Capacity	County	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC

** Note: Non-Band 14 coverage statistics should be broken down by technology: LTE, 3G, 2G, and roaming.

F.4.2.2.2 Deployment Schedule and Status

The Contractor shall provide maps noting the coverage and capacity in rural and non-rural areas and active and planned roaming agreements. The maps shall indicate the then-current coverage (with each monthly submittal) as well as the planned coverage targets for future Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones. The maps shall be provided on a monthly basis for each of the 56 states and territories as well as for the nation as a whole. The Contractor shall also provide a planned deployment schedule and note any changes to the schedule or changes in coverage expectations.

F.4.2.3 Network Technology Roadmap

The Contractor shall provide a network technology roadmap that details vendor equipment capabilities, features, and services identified for inclusion in the NPSBN. For each planned release, the Contractor shall note the targeted availability date and describe the capability, feature, or service, as well as the specific 3GPP release supported. The roadmap shall also note changes in hardware, software, and other network elements impacted by planned releases.

The roadmap shall be provided beginning six (6) months after contract award and subsequent updates shall occur every six (6) months thereafter, unless additional updates are needed and/or mutually agreed upon.

F.4.2.4 Network Operations

The Contractor shall provide the following network operations deliverables post contract award.

F.4.2.4.1 Integration of State-Deployed RANs

The Contractor shall describe the status of efforts to integrate state-deployed RANs. This report shall be provided quarterly beginning three (3) months after award.

F.4.2.4.2 NPSBN Key Performance Indicators

As noted in Section F.4.1, Proposed Deliverables, and Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.1.8, Section Eight – Deliverables Table, the Offeror shall propose deliverables that provide a formal means of communicating the metrics noted in the Quality Assurance Surveillance Plan (QASP). At a minimum, the Contractor shall provide end-to-end performance data of the NPSBN including both Band 14 and non-Band 14 operations (if applicable). The report shall include key performance indicators (KPIs) and trends for the network performance, User Equipment, and services.

This report shall be provided quarterly beginning three (3) months after award.

Measured network KPIs should address the following areas:

- **Accessibility** – Addresses the probability for an end user to be provided with an LTE radio bearer upon request. Measurements include the percentage of successful attempts per overall number of attempts.
- **Retainability** – Addresses how often an end user abnormally loses an LTE radio bearer during the time that the radio bearer is used. Measurements include the percentage of abnormal session releases per session time units.
- **Integrity** – Addresses how the LTE network affects the service quality provided to an end user, or the delay experienced by an end user. Measurements include throughput (Internet Protocol [IP] data volume per time) and latency.
- **Availability** – Addresses when an LTE cell is available for service. Measurements include the percentage of time that the cell is considered available.
- **Mobility** – Addresses how well the LTE mobility functions work. Measurements include the handover success rates.

F.4.2.4.3 Deployable Units and Temporary Coverage Solutions

The Contractor shall provide a report showing the status of providing deployable units, the storage locations of deployable units, and usage data. The Contractor shall note the reason for activation (including National Incident Management System types and planned events), time period in use, and traffic statistics.

This report shall be provided semi-annually beginning six (6) months after award.

F.4.2.5 Transition-Out Plan and Status Reports

At the end of the period of performance—or in the event that the Government terminates this contract for any reason, the Contractor shall submit a written phase-out plan to the COR no later than 90 calendar days prior to the expiration of the contract period, unless otherwise agreed upon. The plan shall detail phase-out activities to assure continuity of operations and the execution of a smooth and timely transition. The plan shall include phase-out training to the successor Contractor at a FirstNet facility or at a location in its vicinity as designated by FirstNet. The Contractor shall permit FirstNet to videotape or otherwise record the phase-out training. FirstNet shall have full intellectual property rights to any phase-out training materials and recordings. Phase-out activities shall be coordinated through the COR. The outgoing Contractor shall submit a weekly status report of phase-out activities to the COR beginning the seventh calendar day following the award of a successor contract until otherwise notified by the COR to discontinue.

F.4.2.6 Monthly Status Report

The Contractor shall provide a monthly status report no later than five (5) calendar days after the end of the month. The Contractor shall include, at a minimum, the following data points within the monthly status report:

- Status of major projects
- Risk summary
    - Status of existing risks and update on mitigation efforts
    - New risks identified during the reporting period, the potential impact of each risk, and the plan (including schedule) to mitigate each risk for each task order

  - Note that the Contractor is responsible for reporting all risks across the enterprise, regardless of whether the risk relates to the Contractor or a teaming partner. The Contractor shall maintain a methodology for identifying and reporting risks across the scope of the contract and subsequent task orders.
- Summary of performance metrics for a rolling six months

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

  - Measurement, for the reporting period and the previous five reporting periods, of items outlined in the Contractor-supplied QASP
  - Approach and steps taken to address measurements that did not meet required thresholds and/or objectives
- Recommendations for mitigation and/or resolution

F.4.2.7 Continual Service Improvement Plan

The Contractor shall provide a continual service improvement (CSI) Plan quarterly, beginning three (3) months after award that includes, at a minimum, the following data points:

- Proposed enhancements to existing processes or services for implementation
- Proposed new processes or services for implementation
- Proposed modifications or enhancements to roles and responsibilities associated with the enhanced or new process(es) or service(s)
- Required automation enhancements to implement the enhanced or new process(es) or service(s)
- Required modifications to or new standard operating procedures for the enhanced or new process(es) or service(s)
- Proposed CSI projects
- High-level timeline to implement each proposed CSI project
- Rough Order of Magnitude (ROM) cost for each proposed CSI project
- Proposed performance metrics in support of each proposed CSI project
- Expected quantitative and qualitative benefits associated with each proposed CSI project and the plan to measure the effectiveness of each proposed project
- Risks associated with each proposed CSI project
- Impact of each proposed CSI project on other process(es) and service(s)

F.4.2.8 Applications Ecosystem

The Contractor shall provide the following applications ecosystem status reports quarterly beginning three (3) months after award.

F.4.2.8.1 Application Programming Interface Taxonomy

The Contractor shall provide a report on network, cloud and data services, and the Application Programming Interfaces (APIs) that are available for application developers to foster new, creative public safety applications.

F.4.2.8.2 Federated Identity

The Contractor shall provide a report on the progress of building the federated FirstNet Identity, Credential, and Access Management (ICAM) trust framework. At a minimum, the report shall include the number of public safety agencies onboarded, the number of unique user identity profiles, and operational metrics.

F.4.2.8.3 FirstNet Applications Store

The Contractor shall provide a report on the progress of building a robust public safety applications marketplace. The report shall, at a minimum, detail the public safety applications published in the FirstNet applications store; the number of applications downloaded; applications ratings from law

enforcement, fire, and emergency medical services users; measures of application life-cycle management; and operational metrics.

F.4.2.8.4 Application Development Platform

The Contractor shall provide a report on the progress of building an application development platform. At a minimum, the report shall include a catalog of the application development tools, APIs, Software Development Kit (SDK) libraries, application frameworks, testing tools, number of registered application developers, and operational metrics.

F.4.2.8.5 Developer and Application Certification

The Contractor shall provide a report on the progress of building a vibrant application developer community and application certification pipeline. The report shall include, at a minimum, the total numbers of certified developers, certified applications, failed certifications, and certification timelines, as well as operational metrics.

F.4.2.8.6 Application Security

The Contractor shall provide a report on the security of user data and applications. At a minimum, the report shall include operational metrics on malware, intrusions, breaches, incidents, and sources of threats.

F.4.2.8.7 Local Control Application

The Contractor shall provide a report on the progress of building and deploying local control capabilities. The report shall include, at a minimum, the total number of trained and certified users and administrators, performance metrics related to latency during provisioning and updating static and dynamic profiles during incidents, and operational metrics.

F.4.2.8.8 Public Safety Entity Home Page

The Contractor shall provide a report on the progress of deploying and driving adoption of the Public Safety Entity (PSE) home page. At a minimum, the report shall include the total number of adopting agencies, agency satisfaction, and operational metrics.

F.4.2.8.9 Application Product Roadmap

The Contractor shall provide a roadmap for expected public safety applications. The report shall include, at a minimum, federated ICAM, local control, network services, the FirstNet applications store, cloud services, the PSE home page, and the application development environment that leverages emerging standards and the commercial marketplace.

F.4.2.8.10 Applications Ecosystem Performance Metrics

The Contractor shall provide a report on the functionality of the applications ecosystem, including, as a minimum, performance, availability, reliability, scalability, resilience, manageability, and security

F.4.2.8.11 Applications Ecosystem Revenue

The Contractor shall provide a report on the business success of the applications ecosystem. At a minimum, the report shall include all applications ecosystem revenue from user fees, application purchases, cloud services, and data services.

F.4.2.9 Device Ecosystem

The Contractor shall provide the following device ecosystem status reports quarterly beginning three (3) months after award.

F.4.2.9.1 Device Summary Report

The Contractor shall provide a summary report of the total number of applications downloaded, the total number of completed over-the-air (OTA) updates, issues with devices and software updates, issues with shared device updates, and bring your own device (BYOD) software updates.

F.4.2.9.2 Universal Integrated Circuit Card Inventory Management

The Contractor shall provide a report that gives the total numbers of active and inactive Universal Integrated Circuit Cards (UICCs) in inventory, assigned/unassigned devices in inventory, and UICC and/or devices that are on order or in the return cycle.

F.4.2.9.3 Applications and Content Management Policies

The Contractor shall provide a report that summarizes updates to applications and content management policies on active devices, including the number of devices that have been successfully updated to align with each policy and how many have failed to update.

F.4.2.9.4 Over-the-Air Status

The Contractor shall provide the total number of OTA updates that have been used for operating system/firmware upgrades, sorted by device model and Original Equipment Manufacturer, as well as the total number devices remaining to be upgraded.

F.4.2.9.5 Diagnostics Monitoring and Management Quality

The Contractor shall provide a summary of devices that have undergone diagnostics, the total number and type of test failures, and the model numbers, sorted by Original Equipment Manufacturer.

F.4.2.9.6 Dedicated Device Software Version Control and Management

The Contractor shall provide the total number of single user devices that have been upgraded to each valid software version, as well as the total number of those that have failed to upgrade.

F.4.2.9.7 Shared Device Software Version Control and Management

The Contractor shall provide the total number of shared devices that have been upgraded to each valid software version, as well as the total number of those that have failed to upgrade.

F.4.2.9.8 Bring Your Own Device Management

The Contractor shall provide the number, vendor, and model of all BYOD devices on the network and the agency or state/territory deploying them.

F.4.2.9.9 Device Inventory and Fulfillment

The Contractor shall provide a list of devices in Contractor's inventory, those on order, and those in the return cycle.

F.4.2.9.10 Subscription Management

The Contractor shall provide a list of active devices and the date they were provisioned and de-provisioned from the network. The report shall include the device model number and type that each user was assigned, sorted by agency.

F.4.2.9.11 Personal Communications Services Type Certification Review Board

The Contractor shall provide a list of all Personal Communications Services (PCS) Type Certification Review Board (PTCRB) certificates that have been supplied by device vendors that have deployed devices on the NPSBN.

F.4.2.10 Business Management

The Contractor shall provide the following business and management reports post award.

F.4.2.10.1 Cost Variance

The Contractor shall provide a monthly report detailing differences between actual and planned network costs as they relate to drawdowns of the budget authority through FOC (this deliverable does not change the Firm Fixed Price of task orders)..

F.4.2.10.2 Revenue Variance

The Contractor shall provide a monthly report detailing differences between actual and planned revenue from use of the network by PSEs.

F.4.2.10.3 Schedule Variance

The Contractor shall provide a monthly report detailing differences in key milestone deliverables relative to the IOC/FOC baseline schedule.

F.4.2.10.4 User Forecasting

The Contractor shall provide a monthly report detailing actual and forecast numbers of device connections (gross add and net add) to the NPSBN. The report shall be broken out by state/territory and provide numbers for the primary user group (i.e., law enforcement, fire, emergency medical services)—by individual disciplines and in total—and the extended primary user group (other public safety users) (see descriptions in Section J, Attachment J-14, Terms of Reference). The report shall also break down the data by pre-paid and post-paid account types.

F.4.2.10.5 Revenue Metrics

The Contractor shall provide a monthly report detailing key device connections (or other relevant metrics). At a minimum, the report shall include the average revenue per user, average revenue per account, average number of devices per account, average usage per device and per account, equipment revenue, applications revenue (to the extent they are invoiced by the Contractor), and average revenue per gigabyte. The metrics shall be broken out by state/territory and provide numbers for the primary user group (i.e., law enforcement, fire, emergency medical services)—by individual disciplines and in total—and the extended primary user group (other public safety users) (see descriptions in Section J, Attachment J-14, Terms of Reference). The report shall also break down the data by pre-paid and post-paid account types.

F.4.2.10.6 Cost Metrics

The Contractor shall provide a monthly report detailing key device connection cost metrics. The report shall include, at a minimum, cash cost per user, cost per gross addition, and customer lifetime value.

F.4.2.10.7 End-User Fee Pricing

The Contractor shall provide a monthly report detailing actual and anticipated end-user fees, pricing adjustments, and promotions.

F.4.2.10.8 Disincentive Mechanism

The Contractor shall provide a public safety device connections report throughout the government fiscal year, on a quarterly basis for the period of performance as part of the disincentive mechanism (as described in Section J, Attachment J-6, Quality Assurance Surveillance Plan, Section 5.3, Disincentive Payments). The report shall include, at minimum, gross activations, gross deactivations, net connections, and total connections. The report shall also break down the data by primary user group (i.e., law enforcement, fire, emergency medical services) and extended primary user group (other public safety users) by device type and monthly data usage at a state/territory level.

F.4.2.10.9 Corporate Financial Reports

The Contractor shall provide the following corporate financial reports:

a) A quarterly report, including an income statement, balance sheet, and cash flow statement for the Contractor within 30 days following the end of the Contractor's quarterly reporting period; and
b) A copy of the Contractor's most recent annual audited financial statements within 120 days Contractor's fiscal year-end.

F.4.2.11 Access Policies Update Report

The Contractor shall communicate any changes to security policies that affect the access policies of PSEs and describe when changes need to be made. This report shall be provided within five (5) days of the end of any month in which changes occur.

F.4.2.12 NPSBN Training Performance Report

The Contractor shall provide the total number of first responders that have been trained (by the Contractor or the PSE) on NPSBN access, services, devices, applications, and procedures broken down by agency. This report shall be provided quarterly beginning three (3) months after award.

F.4.2.13 Hardware and Software Change Management Report

The Contractor shall provide a report outlining the magnitude and effectiveness of all hardware and software changes across the NPSBN. The report shall communicate any major issues encountered, impacts to users, and steps to be taken to minimize user impacts going forward. This report shall be provided quarterly beginning three (3) months after award.

F.4.2.14 Service Availability Report

The Contractor shall provide a report outlining the prior month's service availability by reporting area. The report shall include all critical subsystems, networks, and applications that make up the NPSBN. This report shall be provided quarterly beginning three (3) months after award.

F.4.2.15 Capacity Management Report

The Contractor shall provide a report outlining the current and estimated future service needs compared to actual utilization and allocations of the NPSBN. The report shall address all critical subsystems, networks, and applications that make up the NPSBN. This report shall be provided quarterly beginning three (3) months after award.

F.4.2.16 Business Continuity Testing Report

The Contractor shall provide a report that documents comprehensive business impact analysis, risk assessment, and mitigation testing. This report shall be provided quarterly beginning three (3) months after award.

F.4.2.17 Major Event After Action Report

The Contractor shall provide an after action report, as needed, following a disaster event—natural or man-made—or planned major event. The report shall include lessons learned, and process/protocol improvements to be implemented.

F.4.2.18 Hardware and Software Release Management Report

The Contractor shall provide a report that reviews the prior year's hardware and software rollouts as well as the next year's proposed schedule. The report shall include the primary features and functionalities that will be introduced as well as fixes to major and critical NPSBN issues. This report shall be provided annually beginning six (6) months after award.

F.4.2.19 Support of FirstNet Work with Standards Bodies

The Contractor shall work with and support FirstNet technical standards in support of desired FirstNet current and new Safety related features, services and applications including LTE RAN and Core network modifications necessary for support. This will occur as a collaborative working session on a recurring basis, to be determined after award. As appropriate, the Contractor shall leverage their network vendors for this standards support as well.

The Contractor shall develop supporting technical standards contributions, submit and present at standards meetings, as required and mutually agreed upon with FirstNet. The Contractor shall also attend all necessary standards bodies to support FirstNet including but not limited to 3GPP, OMA, ATIS, etc.

These deliverables will be required throughout the life of the contract.

F.4.2.20 Technical Analysis and Security Review of Security Tools

The Contractor shall provide technical and management support in planning, development and testing of security technologies; provide technical analysis in support of development and test activities for new systems and emerging technologies; facilitate development of future requirements and architectures that enable transition of new systems and technologies into the operational baseline. This support shall be provided as required by FirstNet throughout the life of the contract.

F.4.2.21 Business Continuity/Disaster Recovery Plan

The Contractor shall provide, and maintain, a business continuity of operations plan and a disaster recovery plan to ensure the continuity of the Contractor's business and to provide uninterrupted access to and use of the NPSBN, which will, at a minimum provide uninterrupted access to the NPSBN during

the disaster within the recovery time objectives specified in Section C, Statement of Objectives; Section H, Special Contract and Task Order Requirements; and Section J, Attachment J-10, Cybersecurity.

This deliverable will be required within 30 days of award and annually thereafter.

F.4.2.22 Core Network Design

The Contractor shall provide a Core network design and conduct design reviews as noted in Sections F.4.2.22.1, Preliminary Design; F.4.2.22.2, Preliminary Design Review; F.4.2.22.3, Critical Design; and F.4.2.22.4, Critical Design Review, based on their proposed solution (see Sections L.3.2.2.4, Architecture and Infrastructure; L.3.2.2.5, Operations; and L.3.2.2.6, Security), as incorporated into the resultant award.

F.4.2.22.1 Preliminary Design

The Contractor shall provide, on or before but no later than seven (7) calendar days after award, a written preliminary design for the FirstNet Core network. The preliminary design shall include but is not limited to:

- High-level Core design
- Geo-redundancy strategy
- Identification of network function virtualization (as applicable)
- Preliminary interface description documentation
- Description of Quality of Service, Priority, and Preemption (QPP) strategy
- Preliminary transport design
- Testing strategy
- Preliminary feature description list
- High-level network service platform design
- Voice strategy
- Operational and business support systems
- Public Safety Enterprise Network connectivity
- Core network security design

F.4.2.22.2 Preliminary Design Review

The Contractor shall conduct, on or before but no later than 21 calendar days after award, a preliminary design review (PDR). The PDR shall include a presentation to FirstNet and shall afford FirstNet the opportunity to provide verbal feedback to the Contractor on the design elements presented. In accordance with Section F.4, Meetings, Reports, and Other Deliverables, FirstNet will have approximately 15 working days to review the deliverable and provide written comments back to the Contractor after the conclusion of the PDR. If the deliverable is acceptable, the COR will notify the Contractor; otherwise, comments will be provided for revision/rework.

F.4.2.22.3 Critical Design

The Contractor shall provide, on or before but no later than 45 calendar days after award, a written critical design that incorporates agreed-upon changes as a result of the PDR regarding the preliminary design for the FirstNet Core network. The critical design shall include but is not limited to:

- Detailed Core design documentation
- Type, number, and location of network elements at each redundant data center
- Type, number, and location of every Core network element
- Management and orchestration design (in the event a virtual evolved packet core is proposed)
- Provisioning flow diagrams
- Detailed interface description documentation
- Detailed QPP policy documentation
- Operational and business support systems major subsystems
- Detailed transport design
- Detailed feature description list
- Detailed Core network security design
- Testing plans

F.4.2.22.4 Critical Design Review

The Contractor shall conduct, on or before 60 calendar days after award, a critical design review (CDR). The CDR shall include a presentation to FirstNet and shall afford FirstNet the opportunity to provide feedback to the Contractor on the detailed design prior to implementation. In accordance with Section F.4, Meetings, Reports, and Other Deliverables, FirstNet will have approximately 15 working days to review the deliverable and provide written comments back to the Contractor after the conclusion of the CDR. If the deliverable is acceptable, the COR will notify the Contractor; otherwise, comments will be provided for revision/rework.

F.4.3 Orientation Briefing

Within two (2) days from the date of award, the Contractor shall schedule an orientation briefing/initial strategy session with the Government. Both parties will mutually agree upon the specific date, time, and location of the briefing. The Government does not desire an elaborate orientation briefing nor does it expect the Contractor to expend significant resources in preparation for this briefing. Rather, the intent of the briefing is to initiate the communication process between the Government and the Contractor by introducing key participants and explaining their roles; reviewing communication ground rules; assuring a common understanding of requirements and objectives, goals, constraints, policies, expected benefits, and other relevant background information; and discussing near-term deliverables.

F.5 Other Performance Requirements

F.5.1 Productive Direct Labor Hours

The Contractor can only charge for productive direct labor hours, which are defined as those hours expended by Contractor personnel in performing work under this effort. This does not include sick leave, vacation, government or Contractor holidays, jury duty, military leave, or any other kind of

administrative leave, such as acts of God (e.g., hurricanes, snowstorms, tornadoes), Presidential funerals, or any other unexpected government closures.

F.5.2 Legal Holidays

The following government holidays are normally observed:

- New Year's Day
- Birthday of Martin Luther King, Jr.
- Presidential Inauguration Day (metropolitan DC area only)
- Washington's Birthday
- Memorial Day
- Independence Day
- Labor Day
- Columbus Day
- Veterans Day
- Thanksgiving Day
- Christmas Day

Any other day designated by Federal Statute, Executive Order, and/or Presidential Proclamation may also be observed. When a holiday falls on Saturday or Sunday, it is observed on the adjacent Friday or Monday, respectively.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

F.6 Notice to the Government of Delays

In the event the Contractor:

- Encounters difficulty in meeting performance objectives and/or requirements
- Anticipates difficulty in complying with the contract and/or task orders delivery schedule or any date
- Has knowledge that any actual or potential situation is delaying
- Threatens to delay the timely performance of this contract and/or task orders
- Or otherwise becomes aware of any non-compliance with the terms and conditions of this contract and/or task orders

the Contractor shall immediately notify the CO and COR in writing, giving pertinent details, provided that this data shall be informational only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or date or of any rights or remedies provided by law or under this contract.

If the Contractor fails to respond in a timely manner to any portion of this contract, and/or task orders, the delay will be attributed to the Contractor. Although the period of performance may change due to the delay, FirstNet may be entitled to some form of consideration.

If FirstNet delays performance of this contract, and/or task order, the period of performance and/or price and/or payments to FirstNet may be revised upon mutual agreement between the Government and the Contractor.

F.7 Subcontracting Plan Reports

The Contractor shall submit a report for subcontracting under this particular contract and/or a summary report on subcontracts in all contracts between the Contractor and the Department of the Interior that contain subcontract goals for awards to small businesses, small disadvantaged business concerns, HUB zone businesses, service-disabled veteran-owned small businesses, or woman-owned businesses. Reports will be prepared and submitted electronically in accordance with the instructions at the Electronic Subcontracting Reporting System (eSRS) accessible at www.esrs.gov.

Subcontracting Report for Individual Contracts data (formerly Standard Form 294) is due on the 25th day following the close of the reporting period, unless the contract incorporates the Contractor's approved, annual company-wide or division-wide commercial product plan. Summary Report data (formerly Standard Form 295) is due 30 days after the close of the Government's fiscal year. Paper copies of these reports are no longer required.

Table of Contents

G Contract Administration Data

G.1 General

The contract and all associated task orders will be awarded and administered by the Department of the Interior (DOI), Interior Business Center (IBC), Acquisition Services Directorate (AQD) on behalf of the Department of Commerce and the First Responder Network Authority (FirstNet).

G.2 Authority to Obligate the Government

A Contracting Officer, in accordance with Subpart 1.6 of the Federal Acquisition Regulation (FAR), is the only person authorized to make or approve any changes in any of the objectives and/or requirements of this contract, or subsequent task orders, and notwithstanding any clauses contained elsewhere in this contract, the said authority remains solely with a Contracting Officer. In the event the Contractor makes any changes at the direction of any person other than a Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made as a result thereof. No cost chargeable can be incurred before receipt of a fully executed contract and/or task order(s) or specific authorization from the Contracting Officer.

G.3 Accounting and Appropriation Data

Obligations under the contract will occur at the task order level. Accounting and appropriation data for obligations will be set forth on individual task orders.

G.4 Representatives

Notwithstanding the Contractor's responsibility for management during the performance of this contract, and subsequent task order(s), administration of the contract will require maximum coordination between the Government and the Contractor.

The following subsections describe the roles and responsibilities of individuals who will be the primary points of contact for the Government on matters regarding Indefinite Delivery, Indefinite Quantity (IDIQ) contract and Task Order administration as well as other administrative information, unless otherwise stated in the individual task order(s). The Government may change assignments for this Task Order at any time without prior approval of the Contractor. The Contractor will be notified of the change. The FirstNet NPSBN IDIQ Contract and any Task Order will be administered by the Contracting Officer and Contract Specialist. Written communications shall reference the contract and task order number and shall be mailed to the address below.

G.4.1 Contracting Officer (CO)

Gregory Ruderman
U.S. Department of Interior
Interior Business Center
Acquisition Services Directorate – Herndon
381 Elden Street, Suite 4000
Herndon, VA 20170
Email: Greg_Ruderman@ibc.doi.gov

G.4.2 Contract Specialist

Stephanie Leikach
U.S. Department of Interior
Interior Business Center
Acquisition Services Directorate – Herndon
381 Elden Street, Suite 4000
Herndon, VA 20170
Email: Stephanie_Leikach@ibc.doi.gov

G.4.3 DIAR 1452.201-70 Authorities and Delegations (SEP 2011)

(a) The Contracting Officer is the only individual authorized to enter into or terminate this contract, modify any term or condition of this contract, waive any requirement of this contract, or accept nonconforming work.

(b) The Contracting Officer will designate a Contracting Officer's Representative (COR) at time of award. The COR will be responsible for a technical monitoring of the contractor's performance and deliveries. The COR will be appointed in writing, and a copy of the appointment will be furnished to the Contractor. Changes to this delegation will be made by written changes to the existing appointment or by issuance of a new appointment. The COR for this contract will be appointed upon Task Order award.

(c) The COR is not authorized to perform, formally or informally, any of the following actions:

1. Promise, award, agree to award, or execute any contract, contract modification, or notice of intent that changes or may change this contract;
2. Waive or agree to modification of the delivery schedule;
3. Make any final decision on any contract matter subject to the Disputes Clause;
4. Terminate, for any reason, the Contractor's right to proceed; or
5. Obligate, in any way, the payment of money by the Government.

(d) The Contractor shall comply with the written or oral direction of the Contracting Officer or authorized representative(s) acting within the scope and authority of the appointment memorandum. The Contractor need not proceed with direction that it considers to have been issued without proper authority. The Contractor shall notify the Contracting Officer in writing, with as much detail as possible, when the COR has taken an action or has issued direction

(written or oral) that the Contractor considers to exceed the COR's appointment, within 3 days of the occurrence. Unless otherwise provided in this contract, the Contractor assumes all costs, risks, liabilities, and consequences of performing any work it is directed to perform that falls within any of the categories defined in paragraph (c) prior to receipt of the Contracting Officer's response issued under paragraph (e) of this clause.

(e) The Contracting Officer shall respond in writing within 30 days to any notice made under paragraph (d) of this clause. A failure of the parties to agree upon the nature of a direction, or upon the contract action to be taken with respect thereto, shall be subject to the provisions of the Disputes clause of this contract.

(f) The Contractor shall provide copies of all correspondence to the Contracting Officer and the COR.

(g) Any action(s) taken by the Contractor, in response to any direction given by any person acting on behalf of the government or any Government official other than the Contracting Officer or the COR acting within his or her appointment, shall be at the Contractor's risk.

(End of notice)

G.4.4 Contracting Officer's Representative Authority

As the CO's designated representative, the COR is authorized to act in the stead of the CO to monitor the technical effort being performed under this contract and/or subsequent task order(s) unless otherwise delegated on the subsequent task order(s). The COR must become very familiar with the objectives and/or requirements and communicate with the Contractor to ensure the Contractor is making satisfactory progress in performance. Other than the CO, the COR is the only Government employee who may direct the flow of matters between the Government and the Contractor. Additionally, the COR is limited to directing the flow of technical matters, and no other matters.

A contract is a legally enforceable agreement that sets forth the rights and responsibilities of the parties thereto. If the Contractor deviates from the terms of this contract and/or subsequent task order(s), it is a matter between the Government (represented by the CO) and the Contractor. The COR must therefore keep the CO fully informed so that effective solutions can be applied to problems as soon as they develop. The COR will be required to exercise his/her best judgment to determine what matters deserve the attention of the CO. When in doubt, report the matter to the CO.

COR suggestions to the Contractor about what must be done to fulfill the terms and conditions may lead to unauthorized commitments by the Government for additional compensation or to a release of the Contractor from its obligations under this contract and/or subsequent task order(s). The COR must therefore refrain from communicating with the Contractor about matters that are outside the flow of technical matters. If in doubt, ask the CO. While the COR can and must make technical decisions, the COR may not take any contractual administration actions unless they are clearly authorized by a COR appointment.

1. An appointed/designated COR is authorized and required to:
   a. Inspect and monitor the Contractor's performance to assure technical compliance. Immediately notify the CO of non-compliance, failure to make due progress, or a dispute. The COR should refer all discussions concerning disputed matters to the CO.

b. Inspect and verify satisfactory delivery of all services and products, including the Contractor's reports.
c. Verify efficient and satisfactory performance of work for payment purposes. When contracts/task order(s) contain a warranty or maintenance clause, immediately notify the CO and the Contractor of any deficiencies. After you have completed the notification, monitor the Contractor's response. Notify the CO if the Contractor fails to comply with the requirements in a timely fashion.
d. Within five business days of receiving an invoice or an electronic notification through the Invoice Processing Platform (IPP) (www.ipp.gov) enter on the first page of a paper invoice, or in the appropriate space in IPP for an electronic invoice, the recommended action whether to Approve, Reject or Partially Approve the invoice. The COR must make invoice action recommendations on Debit Invoices and/or Credit Vouchers/Memos before IPP can forward them for CO approval.

2. When exercising COR duties under this appointment, the COR is responsible for:
   a. Knowing and understanding the terms and conditions of this contract and/or subsequent task order(s). Immediately discuss any unclear areas with the CO;
   b. Knowing the scope and limitations of the COR authority and using good judgment, skill, and reasonable care in exercising it;
   c. Protecting privileged and sensitive procurement information;
   d. Monitoring the work site periodically to verify progress and informing the CO of the findings concerning:
      1) Actual performance vs. scheduled performance.
      2) Action needed to restore this effort to schedule;
   e. Implementing the Government Furnished Property/Materials (GFP/M) contract provisions, when applicable. COR responsibilities for GFP/M include: providing the CO with any proposed changes, additions, or deletions to GFP/M; ensuring that delivery is made on time; and inspecting each unit upon its return and notifying the CO of any deficiencies;
   f. Monitoring the results of all required tests within the stated time limitations. The results must be promptly forwarded to the CO. When equipment is delivered to more than one site, ensuring the CO is informed in writing (e.g., e-mail) of delivery and acceptance. Ensuring that equipment is not installed or repaired by Government personnel when the responsibility lies with the Contractor;
   g. Documenting actions taken and decisions that have made as the COR, and maintain adequate records to describe sufficiently the performance of the duties as COR during the life of this contract and/or subsequent task order(s). As a minimum, the COR file should contain copies of the following:
      1) COR appointment memorandum
      2) Contract and Task Order(s) award and any modifications
      3) All correspondence
      4) Records of COR inspections
      5) Records of conversations with the contractor
      6) Invoices and vouchers;
   h. Providing the CO with a copy of any correspondence (including e-mail) sent to the Contractor;

i. Assuring that the Contractor has access to the facility as well as appropriate clearances for personnel to have access to classified or sensitive material, when applicable, as soon as it is determined that access to such material will be required;
j. Reviewing and recommending to the CO approval/disapproval of Contractor's requests for public release of information regarding work being performed under this contract and/or subsequent task order(s);
k. Maintaining current COR certification throughout the appointment. In accordance with Office of Management and Budget memorandum dated September 6, 2011, Subject: The Federal Acquisition Certification for Contracting Officer Technical Representatives, CORs must have a minimum of 40 hours of training and must maintain their skills currency through continuous learning. Twenty-two of the required 40 hours of training hours must cover the essential COR competencies. The remaining 18 hours of the required 40 hours of training should include agency-specific courses, electives, and/or those identified by the COR's supervisor, in consultation with the Contracting Officer, as necessary, for managing a particular contract. To maintain a FAC-COR, CORs are required to earn 40 continuous learning points (CLPs) of skills currency training every two years.
l. Immediately notifying the CO of an impending COR change in order to facilitate a smooth transition and early training of the new COR; and
m. Monitoring the performance and dollars expended on time-and-material and labor- hour type line items or contracts to ensure that they appear to be reasonable for the efforts performed; this includes the type of labor and number of labor hours, travel (including locations, duration, and number of travelers), and types and quantities of material.

The COR shall only authorize or approve contractually funded travel expenses which comply with Federal Travel Regulations or Joint Travel Regulation, as appropriate. As a minimum, the COR must review invoices and any status reports provided by the Contractor to verify that the hours and costs incurred are reasonable in view of the Contractor's effort and deliverables provided. The COR must also review invoices to ensure that the labor rates charged are the same as those set forth in this contract and/or subsequent task order(s).

This contract is covered by the Prompt Payment Act, which subjects the Government to penalties if invoices are not paid in a timely fashion. Penalties are assessed if payment is not made within 30 days after receipt of a proper invoice or final acceptance of the goods or services, whichever is later.

To avoid paying late payment penalties from your program funds, it is important that the COR promptly accept/reject delivered goods or services and immediately certify invoices for payment. Payment, inspection, and acceptance procedures are set forth in this contract and/or subsequent task order(s). Notify the CO immediately if goods or services are rejected. Ensure invoices include proper justification for rejected or partially paid invoices.

The COR must ensure that Contractor employees and consultants with access to Government information technology systems complete the required background investigation process. Prior to granting access to Government applications and systems the COR must verify that Contractor employees and consultants meet the mandatory training requirements of OMB Circular A-130 and 5 CFR Part 930.

The COR may face personal pecuniary liability if he/she commits unauthorized acts that obligate the Government to pay for work that is outside the scope of this contract and/or subsequent task order(s). It is therefore essential for the COR to understand that under the COR appointment, the COR must NOT:

a. Modify the stated terms and conditions or the scope of work in any manner. All such changes must be made in writing by the CO;
b. Award, execute, or agree to any contract, contract modification, accord, task or delivery order, notice of intent, or any similar agreement;
c. Obligate the Government, in any way, to make any payment of money outside the terms and conditions of this contract and/or subsequent task order(s);
d. Make a final decision on any contractual matter that is subject to the Disputes Clause at FAR 52.233-1;
e. Terminate the Contractor's right to proceed, or impose or place a demand upon the Contractor to perform any task or permit any substitution not specifically provided for under this contract and/or subsequent task order(s);
f. Change the period of performance;
g. Authorize purchases not provided for under this contract and/or subsequent task order(s);
h. Authorize the use of overtime;
i. Furnish or authorize the furnishing of Government property, except as required under this contract and/or subsequent task order(s);
j. Direct the activities of any employee of the Contractor, except as specifically provided for under this contract and/or subsequent task order(s);
k. Authorize subcontracting or the use of consultants not already authorized under this contract and/or subsequent task order(s);
l. Grant deviations from or waive any of the terms or conditions under this contract and/or subsequent task order(s); or
m. Make any change that affects price, quality, quantity, delivery, or other terms and conditions under this contract and/or subsequent task order(s).

The COR may not delegate any of the duties or responsibilities assigned to you under this appointment, and should ensure that an Alternate COR is appointed to perform duties in the event of your absence.

An appointment as COR will end on the earliest of the following events:

1. Contract and/or Task Order completion.
2. Contract and/or Task Order termination.
3. Leaving present duty position.
4. The CO's termination of this appointment.

When performing COR duties under a COR appointment, the COR shall maintain an arms-length relationship with the Contractor and consistently strive to protect the interests of the Government. The COR should be particularly attentive to possible violations of the False Claims Amendments Act of 1986 and the Program Fraud Civil Remedies Act of 1986, which involve the submission of false claims or the making of false statements. Similarly, the COR shall avoid any act that may tend to compromise the integrity or apparent integrity of yourself or the Government, or which interferes with the Contractor's right to perform.

Gratuities offered to the COR or any other Government official by any private person or company must be reported to the CO. In the capacity as the COR, the COR is responsible for promptly notifying the CO of any suspected violations of the Gratuities Clause, FAR 52.203-3.

If the COR has or intends to obtain any direct or indirect financial interest which conflicts with your duty to promote and protect the interests of the United States (this includes any discussion of employment with the Contractor), the COR shall immediately advise his/her supervisor and the CO of the conflict. The COR shall also avoid the appearance of any such conflict to maintain public confidence in the Government's conduct of business with the private sector.

G.4.5 Contractor's Representative

The Contractor shall provide a Program Manager to facilitate Government-Contractor communications. The Program Manager shall be the primary technical and managerial interface between the Contractor and CO and the COR identified below. The name of this person, and an alternate or alternates, who shall act for the contractor when the Manager is absent, be designated in writing to the CO. The Program Manager or alternate will have full authority to act for the Contractor on all contract matters relating to daily operations.

The Contractor's designated Program Manager for this contract is:

Name: ***TO BE DETERMINED AT TIME OF AWARD***

Address:

Phone:

Fax:

Email:

The Contractor's designated Program Manager for this contract shall have the authority to make any no-cost contract technical, hiring and dismissal decision, or special arrangements regarding this contract.

The Program Manager shall have full authority to act for the Contractor in the performance of the required services. The Program Manager or a designated representative shall meet with the CO/COR as necessary to maintain satisfactory performance and to resolve any issues pertaining to Government/Contractor procedures. At these meetings, a mutual effort will be made to resolve any and all problems identified. Written minutes of these meetings shall be prepared by the Contractor, signed by the Contractor's designated representative, and furnished to the Government within two (2) workdays of the subject meeting. The Program Manager, and all designated representatives, shall be able to fluently read, write, and speak the English language.

The Program Manager or alternate must be available during normal duty hours, as specified herein and to meet with government personnel within 24 hours notification to discuss problems.

The Program Manager may not be diverted to other projects for 180 consecutive days or more without giving prior written notification to the contracting officer or his representative. Such notification shall include a justification for the diversion, together with information on the proposed substitute in sufficient detail to permit analysis of any potential negative effects on contract performance. No

substitution shall be made without the written consent of the contracting officer; provided, however, that the contracting officer may grant such consent retroactively. Any such substitution of a permanent nature will be made a part of this contract through the issuance of a modification.

When the Project Manager is temporarily unavailable to manage the contract effort for a period longer than 72 hours, including absences due to vacation or illness, the contractor will provide to the COR a written designation of an alternate representative, itemizing any limitations in the alternate's authority.

G.5 Payment for Unauthorized Work

No payments will be made for any unauthorized supplies and/or services, or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor of its own volition or at the request of an individual other than a duly appointed COR. Only a duly appointed Contracting Officer is authorized to change the specifications, terms, and conditions under this contract and/or subsequent task order(s).

G.6 Method of Annual Payment

G.6.1 Payments to the Contractor

The Department of the Interior has adopted the General Services Administration's System for Award Management as its database for contractor information. All payments by the Government under this contract shall be made by electronic funds transfer (EFT). Therefore, the clause at FAR 52.232-33, Payment by Electronic Funds Transfer – System for Award Management, applies and is incorporated by reference in Section I, Contract Clauses, of this contract.

G.6.2 Payments to FirstNet

The FirstNet model includes annual payments from the Contractor to FirstNet. The FAR at 32.601(a)(2) allows the Government to collect amounts due from the Contractor under the terms and conditions of the contract. The Government anticipates collecting Payments to FirstNet (Section B.2.2, State and Territory Task Order(s) – Initial FirstNet-Deployed RAN States) from the Contractor as shown below:

- The first payment to FirstNet will be due two weeks after the state and territory task order award date. The first payment amount will be the proposed year 1 payment in the Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13).
- Each subsequent year's payment will be due two weeks prior to the start of the subsequent Government fiscal year and will continue until all proposed 25 payments in the Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13) have been made or until the end of the 25-year period of performance of the IDIQ contract, whichever occurs first.
- The Offeror's proposed payments are severable at the state level.

FirstNet anticipates utilizing pay.gov to collect annual payments from the Contractor. Pay.gov accepts several forms of payment, including EFT. FirstNet anticipates that Pay.gov will be updated prior to contract award with instructions pertaining to the method for payments from the Contractor to FirstNet. The instructions by which the Contractor shall remit payments to FirstNet will be finalized prior to contract award.

G.6.3 Delayed Payments to FirstNet

The FirstNet model includes annual payments from the Contractor to FirstNet. The FAR at 32.601(a)(2) allows the Government to collect amounts due from the Contractor under the terms and conditions of the contract. The Government anticipates collecting Delayed Payments to FirstNet (see Section B.2.3, State and Territory Task Order(s) – Delayed FirstNet-Deployed RANs), from the Contractor as shown below:

- The first payment to FirstNet will be due two weeks after the state and territory task order award date. The first payment amount will be the proposed year 1 payment in the Delayed Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13).
- Each subsequent year's payment will be due two weeks prior to the start of the subsequent Government fiscal year, and will continue until the end of the 25-year period of performance of the IDIQ contract.
- The last payment amount may be adjusted pro rata to align the Offeror's proposal with the respective Government fiscal year and the end of the 25-year period of performance of the IDIQ contract.
- Due to the timing of the respective state and territory task order awards for the Delayed Payments to FirstNet, all Delayed Payments to FirstNet that were proposed by the Offeror and are beyond the 25-year period of performance of the IDIQ contract will not be required.
- The Offeror's proposed payments are severable at the state level.

FirstNet anticipates utilizing Pay.gov to collect annual payments from the Contractor. Pay.gov accepts several forms of payment, including EFT. FirstNet anticipates that Pay.gov will be updated prior to contract award with instructions pertaining to the method for payments from the Contractor to FirstNet. The instructions by which the Contractor shall remit payments to FirstNet will be finalized prior to contract award.

G.7 Other Administrative Considerations

To promote timely and effective administration, correspondence shall be subject to the following procedures:

a) Technical correspondence (where technical issues relating to compliance with the requirements herein) shall be addressed to the COR with an information copy to the CO.
b) All other correspondence, including invoices, (which proposes or otherwise involves waivers, deviations or modifications to the objectives and requirements, terms or conditions) shall be addressed to the Contracting Officer with an information copy to the COR.

G.8 Department of Commerce Acquisition Regulation

G.8.1 CAR Clauses by Reference

The contract clauses set forth in the following paragraphs of the Department of Commerce Acquisition Regulation (CAR) are incorporated in this contract (marked "X" when applicable) with the same force and effect as though set forth herein in full text. The designated clauses are incorporated as they appear in the CAR on the date of this solicitation/contract, notwithstanding the date referenced.

Table 1 CAR Clauses by Reference

Clause	Title	Date
1352.201-70	Contracting Officer's Authority	MAR 2010

G.8.2 CAR Clauses in Full Text

The contract clauses set forth as follows are the CAR clauses.

G.8.3 CAR 1352.201-72 - Contracting Officer's Representative (COR) (APR 2010)

(a) ____TBD_____ is hereby designated as the Contracting Officer's Representative (COR). The COR may be changed at any time by the Government without prior notice to the contractor by a unilateral modification to the contract. The COR is located at:

_____
_____
_____
Phone Number: _____
E-mail: _____

(b) The responsibilities and limitations of the COR are as follows:

(1) The COR is responsible for the technical aspects of the contract and serves as technical liaison with the contractor. The COR is also responsible for the final inspection and acceptance of all deliverables and such other responsibilities as may be specified in the contract.

(2) The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract price, terms or conditions. Any contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the express written prior authorization of the Contracting Officer. The Contracting Officer may designate assistant or alternate COR(s) to act for the COR by naming such assistant/alternate(s) in writing and transmitting a copy of such designation to the contractor.

(End of clause)

G.8.4 CAR 1352.216-76 Placement of Orders (APR 2010)

(a) The contractor shall provide goods and/or services under this contract only as directed in orders issued by authorized individuals. In accordance with FAR 16.505, each order will include:

(1) Date of order;

(2) Contract number and order number;

(3) Item number and description, quantity, and unit price or estimated cost or fee;

(4) Delivery or performance date;

(5) Place of delivery or performance (including consignee);

(6) Packaging, packing, and shipping instructions, if any;

(7) Accounting and appropriation data;

(8) Method of payment and payment office, if not specified in the contract;

(9) Any other pertinent information.

(b) In accordance with FAR 52.216–18, *Ordering,* the following individuals (or activities) are authorized to place orders against this contract:

_____TBD at award_____
(c) If multiple awards have been made, the contact information for the DOC task and delivery order ombudsman is _not applicable___.

(End of clause)

G.9 Invoice

G.9.1 Electronic Invoicing and Payment Requirements – Invoice Processing Platform (IPP) (APR 2013)

Payment requests must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP).

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions - Commercial Items included in commercial item contracts. The IPP website address is: https://www.ipp.gov.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice [Contracting Officer to edit and include the documentation required under this contract]: The Contractor must use the IPP website to register access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from the Federal Reserve Bank of Boston (FRBB) prior to the contract award date, but no more than 3-5 business days of the contract award date. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email ippgroup@bos.frb.org or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the Contracting Officer with its proposal or quotation.

(End of Local Clause)

G.9.2 Invoice Contents

Any payment under this contract and/or task order(s) to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. The Contractor shall bill either monthly or quarterly, in arrears, in accordance with 31 U.S.C 3324.

The Contractor shall submit a proper invoice in accordance with the IOC/FOC milestones but no more than once monthly. Invoices must identify the fixed price payment to the Contractor for each IOC/FOC milestone accepted, corresponding to the pricing tables in Section B, Supplies or Services and Prices/Costs. To constitute a proper invoice, the invoice must include information and/or attached documentation in accordance with FAR 32.905(b).

Table of Contents

List of Tables

H Special Contract Requirements

H.1 General

The terms and conditions of Section H, Special Contract Requirements, of the First Responder Network Authority (FirstNet) Nationwide Public Safety Broadband Network (NPSBN) contract apply to any task order issued under this contract.

H.2 Department of Commerce Acquisition Regulation

The contract clauses set forth in the following paragraphs of the Department of Commerce Acquisition Regulation (CAR) are incorporated in this contract with the same force and effect as though set forth herein in full text. The designated clauses in Table 1 CAR Clauses are incorporated as they appear in the CAR on the date of this contract, notwithstanding the date referenced.

Table 1 CAR Clauses

Clause	Title	Date
1352.208-70	Restrictions on Printing and Duplicating	APR 2010
1352.209-72	Restrictions Against Disclosure	APR 2010
1352.209-73	Compliance with the Laws	APR 2010
1352.209-74	Organizational Conflict of Interest	APR 2010
1352.216-74	Task Orders	APR 2010
1352.231-71	Duplication of Effort	APR 2010

H.3 Advertising of Award

The Contractor shall not refer to this award in commercial advertising, or similar promotions in such a manner as to state or to imply that the product or services provided is endorsed, preferred, or is considered superior to other products or services by the Department of the Interior (DOI). This includes advertising, or similar promotions, in all forms or electronic, broadcast, and print media.

The Contractor is restricted from reproducing the image(s) of the DOI in any form of commercial advertising, or similar promotion. This includes images of official seals and buildings. The reproduction of official seals and the images of buildings is a matter controlled by regulation and Executive Order. The Contractor shall notify the Contracting Officer in advance of any proposed usage of such symbols.

Any use of FirstNet branding must comply with the terms and conditions specified in Section J, Attachment J-21, Terms and Conditions for the Trademark Use.

H.4 Printing

The Contractor shall not engage in, nor subcontract for, any printing (as that term is defined in Title I of the Government Printing and Binding Regulations in effect on the effective date of this contract) in connection with the performance of work under this contract. Performance of a requirement under this contract involving the reproduction of less than 5,000 production units of any one page, or less than 25,000 production units in the aggregate of multiple pages, will not be deemed to be printing. A production unit is a single sheet, size 8.5 x 11 inches, printed on one side and in only one color.

H.5 Contractor Personnel

H.5.1 Appearance

Contractor personnel shall present a neat appearance and be easily recognized as Contractor employees by wearing a Security Identification Badges at all times while on Government premises. When Contractor personnel attend meetings, answer phones, and work in other situations where their status is not obvious to third parties they must identify themselves as such to avoid creating the impression that they are Government employees.

H.5.2 Contractor Interfaces

As part of the performance of this contract, the Contractor and/or its subcontractors may be required to work with other Contractors supporting FirstNet. Such other Contractors shall not direct this Contractor and/or its subcontractors in any manner. Likewise, this Contractor and/or its subcontractors shall not direct the work of other Contractors in any manner.

The Government shall establish an initial contact between the Contractor and other Contractors and shall participate in an initial meeting at which the conventions for the scheduling and conduct of future meetings/contacts are established. Any CORs of other efforts shall be included in any establishment of conventions.

H.5.3 Warranty against Dual Compensation

The Contractor warrants that any employee who is involved in two or more projects where at least one of which is supported by Federal funds, will not be compensated for more than 100% of his/her time during any part of the period of dual involvement

H.5.4 Key Personnel

Any key personnel applicable to this contract shall be identified herein and/or as specified within the individual task order(s). The following language will be included in each task order that requires key personnel.

The individuals considered essential to the services being provided under this contract and are hereby identified as key personnel as shown in Table 2 Key Personnel:

Table 2 Key Personnel

Name	Position
TBD	Program Manager
TBD	Lead Technical Point of Contact

The Contractor agrees to assign those persons identified above and who are necessary to fulfill the objectives and requirements of the contract as key personnel, and who are approved by FirstNet and DOI. Any key personnel applicable to the individual task orders will be identified within the task order. Any substitution of key personnel will be in accordance with the terms and conditions of this contract, unless otherwise stated.

The following instructions address the procedures for substitution of key personnel:

(a) Resumes for substitutions and/or additions to the Contractor's key personnel shall be submitted for the written approval of the CO. Any substitutions and/or additions shall be subject to the terms and conditions of this contract.

(b) During the first 180 days of performance, no key personnel substitutions shall be permitted unless such substitutions are due to illness, injury, death, disciplinary action, demotion, bona-fide promotion, termination of employment, or other exceptional circumstances when approved by the CO. In any of these events, the Contractor shall promptly notify the CO and provide the information required by paragraph (d) below. After the initial 180-day period, in accordance with paragraph (d) below, all proposed substitutions and additions of key personnel shall be submitted to the CO in writing at least 15 calendar days (30 calendar days if security clearance is to be obtained) prior to the Contractor anticipated effective date of the proposed substitutions and additions.

(c) The CO may consider additional key personnel on an individual basis.

(d) For all requests for substitutions and additions, the Contractor shall provide a detailed explanation of the circumstances requiring the proposed substitution or addition. A complete resume for each proposed substitute or addition, and any other information requested by the CO shall be provided. The Contractor shall certify that the proposed replacement is better qualified than, or at least equal to, the key personnel to be replaced, subject to the penalties in 18 USC 1001. The CO or the CO's authorized representative will evaluate such requests and promptly notify the Contractor of the approval or disapproval thereof.

(e) The Contractors Resource Management Plan submitted as part of the proposal and incorporated as part of this contract shall be updated by the Contractor within 15 calendar days of the receipt of the CO's approval of a substitution or of an addition to the Contractor's key personnel listed above.

H.5.5 Supervision of Contractor Employees

The Contractor shall be responsible for managing and overseeing the activities of all Contractor personnel, as well as subcontractor efforts used in performance of this effort. The Contractor's management responsibilities shall include all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained herein.

If the Contractor finds clarification necessary with respect to the scope of services to be performed or the manner in which the services are to be performed hereunder, the Contractor shall request, in writing, such clarification from the Contracting Officer.

At no time during contract or task order performance shall Contractor personnel be employees of the U.S. Government.

The Contractor's employees and subcontractors shall make clear, in dealings with the public, federal employees, or other contractors that they are not federal employees. To minimize possible confusion, Contractors and subcontractors shall not wear clothing or other items (apart from official identity credential) bearing the name, logo, or seal of the U.S. Government while performing work under this contract or any associated task order.

H.6 Security Requirements

H.6.1 Physical Security

The Contractor shall be responsible for safeguarding all Government assets, information, and property provided for Contractor use. Government equipment and materials must be secured at all times.

H.6.2 Personnel Security Requirements

The Contractor shall provide appropriately cleared Contractor personnel in accordance with the security provisions of this contract. At a minimum, Contractor key personnel administering or maintaining the system(s) shall be required to comply with Homeland Security Presidential Directive 12 (HSPD-12).

Additionally, the Contractor shall comply with all Federal Information Security Management Act (FISMA) standards, which requires Government employees and contractors to be subject to Federal information security laws, regulations and policies, including annual security awareness training.

All Contractor key personnel working on this contract may be requested to be cleared for a Level 2 – non-critical sensitive designation, which encompasses positions designated as moderate risk, non-critical sensitive, and/or to allow access to Confidential information, and Secret information. The Contractor shall provide appropriate personnel who are able to pass the background investigation for access to Government facilities. Background investigations for Level 2 positions consist of the following:

- Submission of fingerprints and a check of appropriate databases for prior federal investigations.
- Corroboration of date and place of birth through appropriate documentation by a trusted information provider.
- e-QIP submission.
- Verification of citizenship or legal resident status of foreign-born applicants.
- Local law enforcement agency checks at all places of employment, residence, or school attendance of six months or more during the past 5 years. Check of the appropriate criminal justice agency for details and disposition of any identified arrest.
- Completed NAC (National Agency Check)
- Expansion of investigation as necessary.

Contractor key personnel may be subject to the same personnel security and suitability requirements as DOC employees and may be required to comply with the same Federal rules and regulations; the governing document for Contractor security investigations is the EO 12829.

Background investigations may be conducted for all Contractor key personnel to determine their suitability to be allowed to work on this contract or any subsequent task order. The Contractor shall provide the information required for such background investigations and shall agree to abide by the DOC DOI personnel security and suitability determination to include EO 12829 upon notification.

H.6.3 Contractor Employee Access

Sensitive Information means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Commerce;
- Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Commerce (including the Assistant Secretary for the National Telecommunication Information Administration or his/her designee);
- Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted security information handling procedures.

"Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

H.7 Restrictions on Future Contracting with FirstNet

The parties to this contract hereby agree the Contractor will be restricted in its future contracting with FirstNet in the manner described herein. Except as specifically stated herein, the Contractor shall compete for FirstNet business on an equal basis with other companies.

If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work, which are to be incorporated into a solicitation, the Contractor may be ineligible to perform the work described within that solicitation as a prime or first-tier subcontractor under the resultant contract. Such restrictions shall remain in effect for three (3) years following completion of work under this contract. FirstNet will not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

The restrictions as stated herein may be waived by the Contracting Officer if it is determined that such restrictions would be detrimental to any Government program.

H.8 Title to Materials

Title to all reports, slides, tapes, file disks, and other items pertaining to the work performed under this contract and/or subsequent task order(s) ("Materials") shall remain with FirstNet upon completion. The Contractor shall transfer to FirstNet the complete copyrights for all materials developed under this contract or any task order. These rights shall allow FirstNet to freely use the subject materials at any time, through any method of projection, transmission, or distribution. All title to such materials shall fully and exclusively be transferred to FirstNet, and the Contractor shall fully cooperate and provide any necessary documentation to effectuate such transfer.

Other than the rights and interests expressly set forth in this contract, FirstNet retains exclusive right, title, and interest (including but not limited to intellectual property rights and licenses, including the Marks as referenced in Section J, Attachment J-21, Terms and Conditions for the Trademark Use) in and to all FirstNet data. FirstNet data includes, without limitation, the results of any processing of FirstNet data that occurs on any Contractor provided system. The Contractor acquires no rights or licenses through this contract (including but not limited to intellectual property rights or licenses) to use FirstNet's data for its own purposes. The Contractor does not acquire and may not claim any security interest in the data.

FirstNet retains the right to access and retrieve its data stored on the Contractor's service infrastructure at its sole discretion and in an accessible (i.e., nonproprietary) format.

FirstNet hereby grants to Contractor, and Contractor hereby accepts from FirstNet, a limited, personal, non-exclusive, non-transferable, non-sublicenseable right and license to use the Materials solely and exclusively in connection with the performance of Contractor's obligations under this contract and/or task orders.

H.9 Disposition of Material

Upon termination or completion of all work under this contract and/or subsequent task order(s), the Contractor shall prepare for shipment, deliver FOB destination, or dispose of all materials received from

the Government (federal or state). If the Government pays for any materials produced or delivered under this contract and/or subsequent task order(s), these materials may become and remain the property of FirstNet.

H.10 Confidentiality of Data

The work under this contract may require access to proprietary, business confidential, or financial data of other companies, states, tribes and/or the Federal Government internal, planning or procurement sensitive/source selection data, which, if released to third parties may give unfair business, technical, or competitive advantages. As long as such data remains proprietary or business confidential, the Contractor shall protect such data from unauthorized use and disclosure and agrees not to use it to compete with such companies or for any purpose other than performance of this contract.

This data may be in various forms, such as documents, or it may be interpretative results derived from analysis, investigative, or study effort. Regardless of the form of this data, the Contractor agrees that neither it nor any of its employees will disclose to third parties any such data, or derivatives thereof, except as may be required in the performance of this contract. Further, the Contractor will not copy any of this data, or derivatives thereof, other than as necessary for the performance of this contract.

The Contractor will establish policies and procedures to implement the substance of this clause at the individual employee level, which will assure that affected employees are made aware of the contract provision and the Contractor's implementing policies and procedures. Particular attention will be given to keeping employees advised of statutes and regulations applicable to the handling of third party confidential or financial data.

This clause does not preclude the Contractor and/or its employees from independently acquiring and using data from legitimate sources outside of this contract, or from performing and using independent analysis of data so acquired, provided that the Contractor and/or its employees fully document the source of such data, and the independence of any such analysis.

The Contractor shall immediately notify, in writing, the Contracting Officer in the event that the Contractor determines or has reason to suspect a breach of this requirement.

The Contractor will insert the substance of this clause in each subcontract hereunder (other than for purchase of supplies or equipment) unless the Contracting Officer has waived this requirement, in writing, as to particular subcontracts or classes of subcontracts.

Any unauthorized disclosure of information may result in termination of this contract for cause.

H.11 Technology Refresh/Enhancement Proposals

During the performance of this contract, the Government may solicit, and at the Contractor's discretion may submit Technology Refresh/Enhancement (TRE) Proposals. TRE means any changes and/or enhancements within the service areas and/or service lines contained in this contract. This may include any products and/or services that are not specified within the contract as long as they are within the general scope. The TRE shall contain the documentation by which any proposed change is described, justified, and submitted to the procuring activity for approval or disapproval. These TREs, must be within the general scope of this contract, may be requested by the Government and/or proposed by the Contractor, for certain objectives and/or requirements specified herein. The TREs may include but are not limited to enhancements, technology refresh or renewal, and/or for any other purpose that present

a system or service performance advantage to FirstNet. Improvement in technology that better provides for the needs of employees/users with disabilities is especially encouraged. Implementation of an approved TRE may occur by either a supplemental agreement or, if appropriate, as a written change order to the contract and/or subsequent task order(s). Additionally, FirstNet considers emergency operations objectives and/or requirements, and any associated support services necessary, to be within scope of this contract. Therefore, any modifications and/or task orders maybe be executed for any objectives and/or requirements within this area. This would include Contractor operation and maintenance of Government owned assets within either Government or Contractor owned and operated facilities.

At a minimum, any proposal submitted by the Contractor pursuant to this clause shall include the following information:

- A statement to the effect that the proposal is being submitted pursuant to this clause;
- A detailed description of the proposed changes;
- A detailed comparison between the existing contract objectives and/or requirements and the proposed changes, including the advantages and disadvantages of each;
- An itemized list of each contract objective and/or requirement, including any delivery schedules or completion dates that would, in the Contractor's opinion, be effected by the proposed changes;
- An estimate of any change (increase or decrease) to the contract's price, including any related cost;
- An estimate of the date by which the Government should accept the proposal in order to receive maximum benefits; and,
- The date until which the proposal is valid. (This date must provide reasonable time for the Government to review the proposal.)

The Contractor may withdraw, in whole or in part, any improvement proposal, which is not accepted by the Government within the specified time for acceptance.

The Contracting Officer shall accept or reject any improvement proposal by giving the Contractor written notice of such acceptance or rejection.

If the proposal is accepted, the Contracting Officer shall issue a contract or task order modification to incorporate any necessary changes, including any increase or decrease in the price. Such adjustment shall be made in accordance with the changes clause of this contract.

Unless and until the contract is modified in writing to incorporate any changes resulting from the Government's acceptance of an improvement proposal, the Contractor shall continue to perform in accordance with the existing terms and conditions.

The Contracting Officer's decision to accept or reject any improvement proposal shall be final and shall not be subject to the terms cited in the disputes clause. Furthermore, the Government shall not be liable for the direct reimbursement of any proposal costs. In no event shall the Government be liable for any additional costs incurred by the Contractor due to the Government's delay in accepting or rejecting any improvement proposal.

The Contractor is requested to identify specifically any information contained in its improvement proposal which it considers confidential and/or proprietary and which it prefers not be disclosed outside the Government. The Contractor's identification of information as confidential and/or proprietary is for

informational purposes only and shall not be binding on the Government. The Contractor is advised that such information may be subject to releases under the Freedom of Information Act (5 U.S.C. 552).

H.12 Indemnity

The Contractor shall hold the Government, its officers, agents and employees, harmless from liability of any nature or kind, including costs and expenses to which they may be subject, for or on account of any or all suits or damages of any character whatsoever resulting from injuries or damages sustained by any person or persons or property by virtue of performance of this contract, arising or resulting in whole or in part from the fault, negligence, wrongful act or wrong mission of the Contractor, or any subcontractor, or their employees, agents, etc., including any failure of Contractor to fully comply with all applicable laws and regulations.

Nothing in paragraph a above shall be considered to preclude the Government from receiving the benefits of any insurance the Contractor may carry which provides for the indemnification of any loss or destruction of, or damages to property in the custody and care of the Contractor where such lass, destruction or damage is the Government property. The Contractor shall do nothing to prejudice the Government's right to recover against third parties for any loss, destruction of, or damage to Government property, and upon the request of the Contracting Officer shall, at the Government's expense, furnish the Government all reasonable assistance and cooperation (including assistance in the prosecution of suit and the execution of instruments of assignment in favor of the Government) in obtaining recovery.

The Contractor agrees to include this clause, appropriately modified, in all subcontracts to be performed under this contract.

H.13 Section 508 Applicable Standards

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), individuals with disabilities must have access to and use of information and data that is comparable to individuals without disabilities. Requirements for accessibility based on Section 508 are determined to be relevant for the NPSBN. A description of the Section 508 standards is located at: http://www.section508.gov/index.cfm?fuseAction=stdsdoc.

The requirements outlined in Table 3 Section 508 Applicable Standards apply to this acquisition.

Table 3 Section 508 Applicable Standards

Section 508 Standard	Title
36 CFR Section 1194.21	Software Applications and Operating Systems
36 CFR Section 1194.22	Web-based Internet Information and Applications
36 CFR Section 1194.23	Telecommunication Products
36 CFR Section 1194.24	Video and Multimedia Products
36 CFR Section 1194.31	Functional Performance Criteria
36 CFR Section 1194.41	Information, Documentation, and Support

H.14 Most Favored Customer Pricing Consideration

To ensure public safety subscribers to the NPSBN pay no more than the lowest price available for any type of customer receiving broadband LTE services on Band 14 or other bands, the Contractor agrees by execution of this contract to provide a most favored customer pricing arrangement to public safety subscribers of NPSBN.

H.15 CAR 1352.227-70 Rights in Data, Assignment of Copyright (APR 2010)

In accordance with 48 CFR 52.227–17, Rights in Data—Special Works, the Contractor agrees to assign copyright to data, including reports and other copyrightable materials, first produced in performance of this contract to the United States Government, as represented by the Secretary of Commerce.

H.16 Bankruptcy and Assurances

H.16.1 Contractor Provisions

Notwithstanding the provisions of Section I, Contract Clauses, (Termination) of this contract, and without prejudice to FirstNet's exercise of any of its other rights under this contract, the Government will have the right, at its sole option, to terminate this contract for cause, suspend performance under this contract, or seek Further Assurances as set forth in Section H.16.5 or require other reasonable actions by the Contractor to provide FirstNet reasonable assurance of its ongoing ability to perform on a sustained and continuous basis if (i) the Contractor's credit rating is reduced by 2 or more steps in any six-month period by any one of the major credit rating agencies, including Moody's investors Services, Standard & Poors, or Fitch, or (ii) the Contractor breaches financial ratio covenants (such ratios to be agreed and calibrated by the Parties as condition of award) in respect of the Contractor's liquidity, profitability and credit strength, or (iii) FirstNet otherwise has reasonable cause to doubt the Contractor's financial stability (including concerns over the Contractor's ability to perform its obligations under any task order consistently and in a sustained manner), or (iv) the Contractor files a petition in bankruptcy or makes a general assignment for the benefit of creditors, or the Contractor has taken any action for the purpose of entering into winding-up, dissolution, bankruptcy, reorganization, or similar proceedings analogous in purpose or effect thereto, or any such action will have been instituted against the Contractor and the Contractor will have acceded thereto or such action will not have been dismissed or stayed within sixty (60) calendar days of the institution thereof, or any order will have been made by any competent court or any resolution will have been passed for the appointment of a liquidator or trustee in bankruptcy or the Contractor will have appointed or suffered to be appointed any receiver or trustee of the whole or any material part of its assets or business.

H.16.2 Failure to Assert Right to Retain Benefits in the Event of Contractor Bankruptcy

In the event Contractor declares bankruptcy, FirstNet may retain its rights under any executory agreement under which the debtor is the licensor of a right to intellectual property pursuant to 11 U.S.C. § 365(n)(1)(B). Any failure of FirstNet to affirmatively notify the Contractor's trustee of its intention to retain its rights under this contract, or any related Agreement, shall not be construed as a termination of this contract, or any related Agreement, pursuant to 11 U.S.C. § 365(n)(1)(A).

H.16.3 No Liens

Except for any security interests in the NPSBN (including all related assets) granted to FirstNet, the Contractor will not cause or permit the NPSBN to become subject to any mechanic's or vendor's lien, or any similar lien or security interest, except as such liens may apply generally to the Contractor's owned infrastructure utilized for the NPSBN (and not to the spectrum capacity particularly) and as are in force as of the Effective Date of this contract. If the Contractor breaches its obligations under this contract, it will immediately notify the Contracting Officer in writing, and the Contractor will promptly take all steps needed to cause such lien to be discharged and released of record without cost to FirstNet.

H.16.4 Transition Plan

In addition to any other transition obligations, upon any termination event under this contract, in addition to any rights afforded to FirstNet under law, at the written notification of FirstNet, the Contractor shall immediately transition the operation of the NPSBN, including the ability to provide Services, to FirstNet, or a third party designated by FirstNet, in accordance with a "Transition Plan," which shall be prepared by the Contractor and approved by FirstNet. The Contractor shall undertake best efforts to cooperate with FirstNet and any subsequent supplier in the smooth transition of all services.

H.16.5 Further Assurances

In connection with this contract and the transactions contemplated hereby, each party will execute and deliver any additional documents and instruments and perform any additional acts that may be commercially reasonable, necessary, or appropriate, or reasonably requested by the other party, to effectuate and perform the parties' obligations under this contract and the transactions contemplated hereby.

H.16.6 Business Continuity/Disaster Recovery Plan

The Contractor will at its sole expense, establish and maintain a business continuity/Disaster Recovery plan to ensure the continuity of the Contractor's business and to provide uninterrupted access to and use of the NPSBN, which will, at a minimum, contain: (1) written disaster recovery plans for critical technology and infrastructure, including the NPSBN; (2) proper risk controls to enable continued performance under this contract in the event of a disaster; (3) procedures that will be invoked in the occurrence of a Force Majeure Event; and (4) demonstrated capability to provide uninterrupted access to the NPSBN during the disaster within the recovery time objectives specified in Section C, Statement of Objectives.

H.17 Notice of Supply Chain Risk Assessment

In accordance with the language provided below and as stated herein, FirstNet reserves the right to conduct a Supply Chain Risk Assessment (SCRA) of the equipment/devices and software/applications under this contract using the information provided by the Contractor as well as other available information, in conducting its assessment.

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

H.18 Organizational Conflict of Interest

The Contractor warrants that, to the best of its knowledge and belief, it does not have any organizational conflict of interest as defined below.

The term "organizational conflict of interest" means a situation where a Contractor or one of its employees has interests, either due to its other activities or its relationships with DOI, DOC or FirstNet, which place it in a position that it is unable or potentially unable, from the Government's standpoint, to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired.

The Contractor agrees that if, after award of the IDIQ contract or any task order award, it discovers an organizational conflict of interest with respect to this contract and/or task order, the Contractor shall make an immediate and full disclosure in writing to the Contracting Officer that shall describe in detail the conflict (or potential conflict) as well as include a description of the action that the Contractor has taken or proposes to take to avoid, mitigate or neutralize the conflict. DOI may, however, terminate this task order for the convenience of the Government if termination is determined to be in the best interest of the Government.

If the Contractor was aware of organizational conflict (or potential conflict) of interest before task order award and intentionally did not disclose the conflict to the Contracting Officer, DOI may terminate this contract and/or task order at no cost to the Government.

H.19 Government-Furnished Property, Facilities, Equipment, and Information

For the purpose of this contract, the Contractor shall assume there is no Government-Furnished Property (GFP); however, should a situation arise, the Government may elect to provide GFP after contract award, or with any subsequent task order(s).

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

GFP is a broad term to include facilities (GFF), equipment (GFE), and/or information (GFI). GFI is considered to include software and data. Any GFP furnished by the Government or acquired by the Contractor must be specified in the contract and/or applicable task order. Contractor acquired property shall be acquired only after the acquisition receives the concurrence of the Contracting Officer's Representative (COR) and the written authorization of the Contracting Officer (CO).

The CO and COR are responsible for ensuring that the contract and all applicable task orders are consistent with the policies and procedures of FAR Part 45 for providing government property to contractors, contractors' use and management of government property, and reporting, redistributing, and disposing of contractor inventory. Contractors are responsible and liable for Government property in their possession pursuant to FAR 52.245-1 and 52.245-2, as applicable.

In the event that the Contactor is notified of the Government's intent to provide GFP and the GFP is not received by the date specified by the Government, the Contractor will immediately notify the COR and CO. If provided, the Contractor shall use the GFP only in connection as specified and associated with this contract and/or task order(s).

At the completion of a task order, all GFP related to that order shall be returned to the Government unless authorization is given by the CO that the GFP is to be used on another task order under this contract. Not later than the completion of this contract, the Contractor shall prepare for return to the Government all GFP in good condition, ordinary wear and tear excepted. Within thirty (30) calendar days of completion of this contract, the Contractor shall submit an Inventory Schedule of residual GFP in a form acceptable to the Contracting Officer. The Contractor shall follow the instructions of the Contracting Officer regarding the disposition of any GFP.

H.19.1 Management of Government Furnished Property

If GFP is provided under this contract, the Contractor shall acknowledge receipt of the GFP and shall assume the risk and responsibility for loss, repair, upgrade, and replacement while the GFP is in the Contractor's possession. Additionally, the Contractor shall maintain a detailed inventory accounting system for all GFP and provide the COR or CO with the status of GFP at any time upon request. The inventory system shall identify track and identify the following information (at a minimum):

- Item name
- description
- Make, model number and serial number
- Date of receipt
- Organization and person received from
- Location
- Condition

H.20 NEPA Compliance

The Contractor shall comply with all applicable environmental and historic preservation laws and regulations (collectively, "Environmental Requirements"). Environmental Requirements include, without limitation, any statute, law, act, ordinance, rule, regulation, order, decree, permit, or ruling of any federal, State, and/or local government, or administrative regulatory body, agency, board, or commission or a judicial body, relating to the protection of human health and/or the environment or historic preservation and otherwise regulating and/or restricting the management, use, storage, transportation, treatment, disposal, and/or any release of a hazardous substance, hazardous waste,

pollutant, or other material. These Environmental Requirements include, but are not limited to, the National Environmental Policy Act (NEPA), the National Historic Preservation Act (NHPA), the Endangered Species Act (ESA), the Migratory Bird Treaty Act, and the Bald and Golden Eagle Act. The Contractor will provide any documentation necessary, or as otherwise requested by FirstNet, to comply with any Environmental Requirements for FirstNet review and approval prior to commencing activities specifically being taken under the terms of any final agreement between FirstNet and the Contractor. Contractor agrees to comply with FirstNet reasonably procedures to ensure FirstNet is able to fully and timely comply with its obligations under NEPA and other applicable Environmental Requirements.

The Contractor shall be the party of record for all permits related to operating the NPSBN and shall be solely responsible for obtaining any new or revised permits needed to operate and maintain the NPSBN. Recognizing that delays in obtaining permits may result in delays to the deployment schedule, and in the spirit of the June 14, 2012 Executive Order "Accelerating Broadband Infrastructure Deployment," the Government will, at its discretion, reasonably assist in the resolution of appropriate permitting issues with federal, state, and local permitting authorities. The Contractor may request Government assistance whenever it encounters delays that may impact its deployment schedule. The Contractor will employ its best efforts to promptly notify the Government when such assistance may be necessary or reduce unanticipated delays.

H.21 FirstNet Auditing

The Contractor shall make all its records—as defined in FAR 52.215-2, Audit and Records—Negotiation (Oct 2010), which is contained in Section I, Contract Clauses—available for inspection by FirstNet and its designees.

H.21.1 Audits

FirstNet shall have such rights to review and audit the Contractor and its records as and when FirstNet deems necessary for purposes of verifying compliance with the Contract and applicable law and verifying claims. Without limiting the foregoing:

- The audits may be performed by employees of FirstNet or by an auditor under contract with FirstNet;
- The Contractor shall allow auditor(s) access to such records during normal business hours, allow interviews of any employee who might have information related to such records, and otherwise cooperate with the auditors; and

H.21.2 Conduct of Audits

Audits conducted under this Section H.21, FirstNet Auditing, will be conducted in accordance with FAR 52.215-2 Audit and Records – Negotiation (Oct 2010) as contained in Section I, Contract Clauses.

H.21.3 Rights of Observation

FirstNet's rights of audit include the right to observe the business operations of the Contractor to confirm the accuracy of records.

H.21.4 Contract Documents

- The Contractor shall establish internal procedures to facilitate review and audit by FirstNet, upon request.
- The Contractor represents and warrants the completeness and accuracy in all material respects of all information it or its agents provide in connection with FirstNet audits.
- The Contractor shall establish internal and third-party quality and compliance auditing procedures.

H.21.5 Flow-Down Requirements

The Contractor shall insert a clause containing all the terms of this clause H.21, FirstNet Auditing, including this paragraph H.21.5, Flow-Down Requirements, in all subcontracts and must contain the clause at FAR 52.215-2, Audit and Records – Negotiation (Oct 2010) as contained in Section I, Contract Clauses.

H.22 FirstNet Inspections

In addition to the rights granted under FAR 52.246-4, Inspection of Services—Fixed-Price (Aug 1996), included in Section E, Inspection and Acceptance, and other sections of this Contract, the Government or its designee shall have the right, until three years after final payment under this contract, to inspect the Contractor's processes, policies, systems, facilities (including but not limited to network facilities) and other materials reasonably deemed by the Government as appropriate to monitor and ensure compliance of the Contractor and its subcontractors with this Contract, the FCC's rules, policies and guidelines, state and local rules and regulations and other applicable law. The Contractor is responsible for its costs related to inspections under this provision, including inspections of Contractor's subcontractors. If any inspection reveals an error or irregularity, in addition to any other rights the Government may have under this contract, including the right to declare Contractor in breach of this contract, the Contractor shall rectify such irregularities within the timeframe established by the Government. The Contractor shall insert a clause containing all the terms of this clause H.22, FirstNet Inspections, in all subcontracts that exceed the simplified acquisition threshold.

Table of Contents

I Contract Clauses

I.1 52.252-2 Clauses Incorporated by Reference (FEB 1988)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

- FAR Clauses: http://www.acquisition.gov/comp/far/loadmainre.html
- CAR Clauses: http://farsite.hill.af.mil/vfcara.htm
- DIAR Clauses: http://farsite.hill.af.mil/vfdiara.htm

Table 1 FAR Clauses Incorporated by Reference

Clause	Title	Date
52.202-1	Definitions	NOV 2013
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government	SEPT 2006
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct	APR 2010
52.203-14	Display of Hotline Poster(s)	DEC 2007
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-4	Printed or Copied Double-Sided on Recycled Paper	MAY 2011
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	JUL 2013
52.204-13	System for Award Management Maintenance	JUL 2013
52.204-15	Service Contract Reporting Requirements for Indefinite Delivery Contracts	JAN 2014
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	AUG 2013
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	DEC 2014
52.210-1	Market Research	APR 2011

Clause	Title	Date
52.211-5	Material Requirements	APR 2000
52.211-11	Has been incorporated in full text; see Section I.4.1, 52.211-11 Liquidated Damages—Supplies, Services, or Research and Development (SEP 2000)	SEP 2000

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Clause	Title	Date
52.215-2	Audit and Records – Negotiation	OCT 2010
52.215-8	Order of Precedence--Uniform Contract Format	OCT 1997
	[Clause removed in its entirety]	
	[Clause removed in its entirety]	
52.215-12	Subcontractor Certified Cost or Pricing Data	OCT 2010
52.215-13	Subcontractor Certified Cost or Pricing Data – Modifications	OCT 2010
52.215-14	Integrity of Unit Prices	OCT 2010
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data—Modifications	OCT 2010
52.217-8	Option to Extend Services	NOV 1999
52.219-4	Notice of Price Evaluation Preference for HUBZone Small Business Concerns	OCT 2014
52.219-8	Utilization of Small Business Concerns	MAY 2014
52.219-9	Small Business Subcontracting Plan ALTERNATE II – OCT 2001	OCT 2015
52.219-16	Liquidated Damages—Subcontracting Plan	JAN 1999
52.222-20	Contracts for Materials, Supplies, Articles, and Equipment Exceeding $15,000	MAY 2014
52.222-3	Convict Labor	JUN 2003
52.222-4	Contract Work Hours and Safety Standards Act—Overtime Compensation Remedies	MAY 2014
52.222-21	Prohibition of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	APR 2015
52.222-37	Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, & Other Eligible Veterans	JUL 2014
52.222-40	Notification of Employee Rights under the National Labor Relations Act	DEC 2010
52.222-50	Combat Trafficking in Persons	
52.222-54	Employment Eligibility Verification	
52.222-55	Minimum Wages Under Executive order 13658	DEC 2014
52.223-2	Affirmative Procurement of Biobased Products Under Service and Construction Contracts	SEP 2013
52.223-14	Acquisition of EPEAT®-Registered Televisions	JUN 2014
52.223-17	Affirmative Procurement of EPA-designated Items in Service and Construction Contracts	MAY 2008
52.223-5	Pollution Prevention and Right-to-Know Information	MAY 2011
52.223-6	Drug-Free Workplace	MAY 2001
52.223-10	Waste Reduction Program	MAY 2011
52.223-13	Acquisition of EPEAT® - Registered Imaging Equipment	JUN 2014
52.223-15	Energy Efficiency in Energy-Consuming Products	DEC 2007
52.223-16	Acquisition of EPEAT® -Registered Personal Computer Products	JUN 2014

Clause	Title	Date
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	AUG 2011
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.225-25	Prohibition on Contracting with Entities Engaging in Sanctioned Activities Relating to Iran—Representation and Certification	DEC 2012
52.227-1	Authorization and Consent	DEC 2007
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	DEC 2007
52.227-3	Patent Indemnity	APR 1984
52.227-14	Rights in Data—General (applicable to other than Special Works) Alternate II – DEC 2007	DEC 2007
52.227-17	Rights in Data—Special Works	DEC 2007
52.227-19	Commercial Computer Software License	DEC 2007
52.227-22	Major System -- Minimum Rights	JUN 1987
52.228-5	Insurance—Work on a Government Installation	JAN 1997
52.229-3	Federal, State, and Local Taxes	FEB 2013
52.232-1	Payments	APR 1984
52.232-6	Payments Under Communication Service Contracts with Common Carriers	APR 1984
52.232-7	Payments under Time-and-Materials and Labor-Hour Contracts	AUG 2012
52.232-8	Discount for Prompt Payment	FEB 2002
52.232-9	Limitation on Withholding of Payments	APR 1984
52.232-11	Extras	APR 1984
52.232-17	Interest	MAY 2014
52.232-23	Assignment of Claims	MAY 2014
52.232-25	Prompt Payment	JUL 2013
52.232-33	Payment by Electronic Funds Transfer-- Central Contractor Registration	JUL 2013
52.239-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.233-1	Disputes--Alternate I	DEC 1991
52.233-3	Protest After Award	AUG 1996
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-2	Protection of Government Buildings, Equipment and Vegetation	APR 1984
52.237-3	Continuity of Services	JAN 1991
52.239-1	Privacy and Security Safeguards	AUG 1996
52.242-1	Notice of Intent to Disallow Costs	APR 1984
52.242-3	Penalties for Unallowable Costs	MAY 2014
52.242-4	Certification of Final Indirect Costs	JAN 1997
52.242-13	Bankruptcy	JUL 1995
52.243-1	Changes—Fixed Price Alternate II (APR 1984)	AUG 1987

Clause	Title	Date
52.243-3	Changes—Time-and-Materials or Labor-Hours	SEPT 2000
52.243-7	Notification of Changes	APR 1984
52.244-2	Subcontracts	OCT 2010
52.244-5	Competition in Subcontracting	DEC 1996
52.244-6	Subcontracts for Commercial Items	APR 2015
52.245-1	Government Property	APR 2012
52.245-9	Use and Charges	APR 2012
52.246-19	Warranty of Systems and Equipment under Performance Specifications or Design Criteria	MAY 2001
52.247-1	Commercial Bill of Lading Notations	FEB 2006
52.248-1	Value Engineering	OCT 2010
52.249-2	Termination for Convenience of the Government (Fixed Price)	APR 2012
52.249-8	Default (Fixed-Price Supply and Service)	APR 1984
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012
52.253-1	Computer Generated Forms	JAN 1991

I.2 Department of the Interior Acquisition Regulation (DIAR)

The contract clauses set forth in the following paragraphs of the Department of the Interior Acquisition Regulation (DIAR) are incorporated in this contract with the same force and effect as though set forth herein in full text. The designated clauses are incorporated as they appear in the DIAR on the date of this contract, notwithstanding the date referenced. The clauses may be viewed at: http://farsite.hill.af.mil/vfdiara.htm

Table 2 DIAR Clauses Incorporated

Clause	Title	Date
1452.203-70	Restriction on Endorsements – Department of the Interior (DIAR)	JUL 1996
1452.215-70	Examination of Records by the DOI	APR 1984
1452.228-70	Liability Insurance—DOI	

I.3 Department of Commerce Acquisition Regulation (CAR)

The contract clauses set forth in the following paragraphs of the Department of Commerce Acquisition Regulation (CAR) are incorporated in this contract with the same force and effect as though set forth herein in full text. The designated clauses are incorporated as they appear in the DIAR on the date of this contract, notwithstanding the date referenced. The clauses may be viewed at: http://farsite.hill.af.mil/vfcara.htm

Table 3 CAR Clauses Incorporated

Clause	Title	Date
1352.201-70	Contracting Officers Authority (CAR)	APR 2010
1352.209-72	Restrictions Against Disclosure	APR 2010
1352.209-73	Compliance with the Laws	APR 2010
1352.209-74	Organizational Conflict of Interest	APR 2010
1352.239-72	Security Requirements for Information Technology Resources	DEC 1994

I.4 Federal Acquisition Regulation

The contract clauses set forth as follows are the Federal Acquisition Regulation (FAR) clauses.

I.4.1 52.211-11 Liquidated Damages—Supplies, Services, or Research and Development (SEP 2000)

(a) If the Contractor fails to deliver the supplies or perform the services within the time specified in this contract, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of $238,233.00 (but the total aggregate amount of the liquidated damages under this clause shall not exceed $86,955,057.00) per calendar day of delay.

(b) If the Government terminates this contract in whole or in part under the Default—Fixed-Price Supply and Service clause, the Contractor is liable for liquidated damages accruing until the Government reasonably obtains delivery or performance of similar supplies or services. These liquidated damages are in addition to excess costs of repurchase under the Termination clause.

(c) The Contractor will not be charged with liquidated damages when the delay in delivery or performance is beyond the control and without the fault or negligence of the Contractor as defined in the Default—Fixed-Price Supply and Service clause in this contract.

(End of clause)

I.4.2 FAR 52.216-18 Ordering (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from contract throughout the life of the contract.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of Clause)

I.4.3 FAR 52.216-19 Ordering Limitations (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $3,500, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor --

(1) Any order for a single item in excess of unlimited dollar value;

(2) Any order for a combination of items in excess of unlimited dollar value; or

(3) A series of orders from the same ordering office within zero days that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within one (1) days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

I.4.4 FAR 52.216-22 Indefinite Quantity (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after expiration of the current period of performance of the IDIQ contract or individual order, whichever is later.

(End of Clause)

I.4.5 FAR 52.219-28 Post-Award Small Business Program Representation (JUL 2013)

(a) Definitions. As used in this clause--

Long-term contract means a contract of more than five years in duration, including options. However, the term does not include contracts that exceed five years in duration because the period of

performance has been extended for a cumulative period not to exceed six months under the clause at 52.217-8, Option to Extend Services, or other appropriate authority.

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (c) of this clause. Such a concern is "not dominant in its field of operation" when it does not exercise a controlling or major influence on a national basis in a kind of business activity in which a number of business concerns are primarily engaged. In determining whether dominance exists, consideration shall be given to all appropriate factors, including volume of business, number of employees, financial resources, competitive status or position, ownership or control of materials, processes, patents, license agreements, facilities, sales territory, and nature of business activity.

(b) If the Contractor represented that it was a small business concern prior to award of this contract, the Contractor shall re-represent its size status according to paragraph (e) of this clause or, if applicable, paragraph (g) of this clause, upon the occurrence of any of the following:

(1) Within 30 days after execution of a novation agreement or within 30 days after modification of the contract to include this clause, if the novation agreement was executed prior to inclusion of this clause in the contract

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

.

(2) Within 30 days after a merger or acquisition that does not require a novation or within 30 days after modification of the contract to include this clause, if the merger or acquisition occurred prior to inclusion of this clause in the contract.

(3) For long-term contracts—

(i) Within 60 to 120 days prior to the end of the fifth year of the contract; and

(ii) Within 60 to 120 days prior to the date specified in the contract for exercising any option thereafter.

(c) The Contractor shall re-represent its size status in accordance with the size standard in effect at the time of this re-representation that corresponds to the North American Industry Classification System (NAICS) code assigned to this contract. The small business size standard corresponding to this NAICS code can be found at http://www.sba.gov/content/table-small-business-size-standards.

(d) The small business size standard for a Contractor providing a product which it does not manufacture itself, for a contract other than a construction or service contract, is 500 employees.

(e) Except as provided in paragraph (g) of this clause, the Contractor shall make the representation required by paragraph (b) of this clause by validating or updating all its representations in the Representations and Certifications section of the System for Award Management (SAM) and its other data in SAM, as necessary, to ensure that they reflect the Contractor's current status. The Contractor shall notify the contracting office in writing within the timeframes specified in paragraph (b) of this clause that the data have been validated or updated, and provide the date of the validation or update.

(f) If the Contractor represented that it was other than a small business concern prior to award of this contract, the Contractor may, but is not required to, take the actions required by paragraphs (e) or (g) of this clause.

(g) If the Contractor does not have representations and certifications in SAM, or does not have a representation in SAM for the NAICS code applicable to this contract, the Contractor is required to complete the following representation and submit it to the contracting office, along with the contract number and the date on which the representation was completed:

The Contractor represents that it [ ] is, [ ] is not a small business concern under NAICS Code _____ assigned to contract number _____.[Contractor to sign and date and insert authorized signer's name and title].

(End of clause)

I.4.6 FAR 52.222-35 Equal Opportunity for Veterans (JUL 2014)

(a) Definitions. As used in this clause--

"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran,' and "recently separated veteran" have the meanings given at FAR 22.1301.

(b) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of $100,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate of identify properly the parties and their undertakings.

(End of Clause)

I.4.7 FAR 52.222-36 Equal Opportunity for Workers with Disabilities (JUL 2014)

(a) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60.741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of $15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

(End of Clause)

I.4.8 FAR 52.224-1 Privacy Act Notification (JUL 1996) (Deviation)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C.552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

Applicable Department of the Interior regulations concerning the Privacy Act are set forth in 43 CFR 2, subpart D. The CFR is available for public inspection at the Departmental Library, Main Interior Bldg., 1849 C St. NW, Washington DC, at each of the regional offices of bureaus of the Department and at many public libraries.

(End of Clause)

I.4.9 FAR 52.252-6 – Authorized Deviation in Clauses (FEB 1998)

(a) Any data required to be submitted on a Standard or Optional Form prescribed by the Federal Acquisition Regulation (FAR) may be submitted on a computer generated version of the form, provided there is no change to the name, content, or sequence of the data elements on the form, and provided the form carries the Standard or Optional Form number and edition date.

(b) Unless prohibited by agency regulations, any data required to be submitted on an agency unique form prescribed by an agency supplement to the FAR may be submitted on a computer generated version of the form provided there is no change to the name, content, or sequence of the data elements on the form and provided the form carries the agency form number and edition date.

(c) If the Contractor submits a computer generated version of a form that is different than the required form, then the rights and obligations of the parties will be determined based on the content of the required form.

(End of Clause)

I.5 Department of the Interior Acquisition Regulation (DIAR)

The contract clauses set forth as follows are the Department of the Interior Acquisition Regulation (DIAR) clause.

I.6 Department of Commerce Acquisition Regulation (CAR)

The contract clauses set forth as follows are the Department of Commerce Acquisition Regulation (CAR) clauses.

I.6.1 1352.216-76 Placement of Orders (APR 2010)

(a) The contractor shall provide goods and/or services under this contract only as directed in orders issued by authorized individuals. In accordance with FAR 16.505, each order will include:

(1) Date of order;

(2) Contract number and order number;

(3) Item number and description, quantity, and unit price or estimated cost or fee;

(4) Delivery or performance date;

(5) Place of delivery or performance (including consignee);

(6) Packaging, packing, and shipping instructions, if any;

(7) Accounting and appropriation data;

(8) Method of payment and payment office, if not specified in the contract;

(9) Any other pertinent information.

(b) In accordance with FAR 52.216–18, Ordering, the following individuals (or activities) are authorized to place orders against this contract:

(c) If multiple awards have been made, the contact information for the DOC task and delivery order ombudsman is not applicable.

(End of clause)

I.7 RESERVED

Section J contains the attachments below.

Reference	Title	Page Count
J-1	Coverage and Capacity Definitions	11
	Coverage Maps: • Coverage_Objectives_Map_v1.0 • Urban-Rural_Map_v1.0 • 2010_Pop_Map_v1.0 • Device_Demand_Map_v1.3 • Tonnage_Demand_Map_v1.3 • User_Demand_Map_v1.3	N/A
J-2	Nationwide and Rural Coverage Compliance Checklist	2
J-3	FCC TAB RMTR	100
J-4	System and Standards Views	24
J-5	Proposal Questions Template	1
J-6	Quality Assurance Surveillance Plan	17
J-7	Operational Architecture	17
	Operational Architecture – Visio File	1
J-8	IOC/FOC Target Timeline	22
J-9	QASP Surveillance Matrix Template	4
J-10	Cybersecurity	18
J-11	Device Specifications Template	N/A
J-12	Test Strategy Template	31
J-13	Pricing Template	N/A
J-14	Terms of Reference	20
J-15	Contractor-Furnished Equipment	2
J-16	Deliverables Table	2
J-17	Coverage and Capacity Template	N/A
J-18	Delivery Mechanism Objectives for State Plans	2
J-19	State Plan Template	42
J-20	Terms and Conditions for the Use of FirstNet Network Capacity	6
J-21	Terms and Conditions for the Trademark Use	4
J-22	Solicitation Conformance Traceability Matrix	3
J-23	End-User Pricing Tables	3
J-24	Public Safety Device Connections Template	N/A
J-25	Past Performance Reference Information Form	3
J-26	Sample Small Business Subcontracting Plan	7
J-27	Parental Guarantee Agreement	6
TOTAL PAGE COUNT		348

Table of Contents

List of Figures

1 Coverage Objectives

The First Responder Network Authority (FirstNet) created a coverage objective map to identify areas where public safety desires persistent coverage and temporary coverage solutions. The map (Figure 1 Coverage Objective Map) includes input from individual states, territories, and tribal nations, when available.

The coverage objective map depicts a one-square-mile grid block for each of the 56 states and territories. The coverage objective map, which covers each of the 56 states and territories, is included within Section J, Attachment J-1 as a shapefile (file titled "Coverage_Objectives_Map_v1.0_AMEND 003.mpk").

The coverage objective map reflects coverage objectives based on data from the following four categories:

- **FirstNet Baseline** – Original coverage objective map developed by FirstNet, further described in Section 3, Coverage Objective Map Methodology.
- **State Inputs** – Areas of interest identified by states, territories, and tribal nations that were not addressed in FirstNet's baseline.
- **Federal Inputs** – Areas of interest from federal entities, not identified by the FirstNet baseline or state inputs.
- **On-Demand Temporary** – Areas where there are rare occurrences for the need of coverage.

The FirstNet baseline, as modified by state and federal inputs, indicates areas where persistent coverage is desired. On-demand temporary solutions are adequate for the other areas identified.

The following values are stored as numbers in the attribute table as opposed to text strings for ease of data manipulation.

"State-Local" Attribute Column

- 0 – None (not identified in FirstNet baseline or in State Input)
- 1 – FirstNet Original Baseline
- 2 – State Input
- 3 – State Input LMR or Commercial Coverage

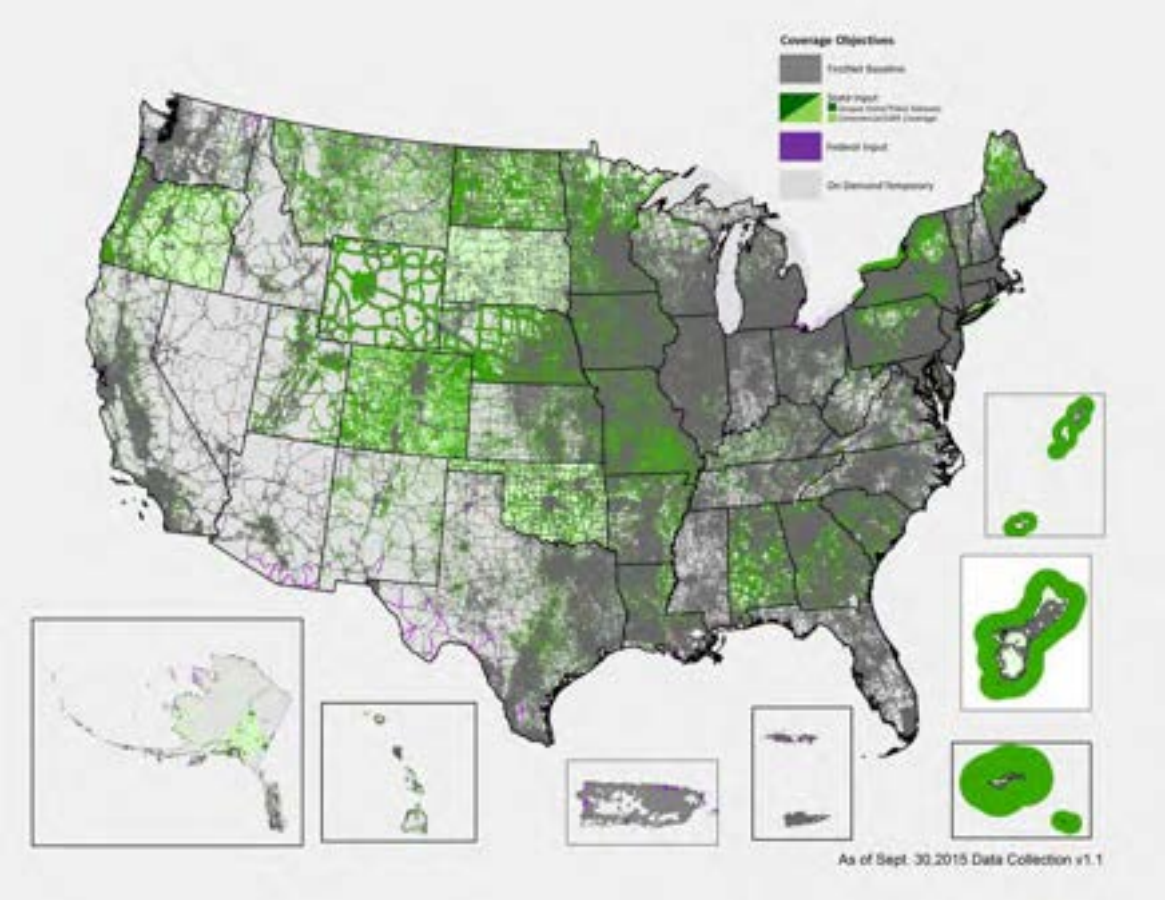


Figure 1 Coverage Objective Map

2 Coverage Definition

Coverage is defined as the geographic area where a base station and mobile device can reliably communicate with each other above a minimum designed data rate.

Persistent and temporary coverage is defined as a Long Term Evolution (LTE) Band 14 network capable of providing cell edge data rates of 256 kbps uplink (UL) and 768 kbps downlink (DL) measured from outdoor stationary User Equipment at three (3) feet from ground level with a 95 percent confidence margin for the cell area with a uniform cell load of 50 percent for the DL and UL. The link budget cell edge data rates (256 kbps UL/768 kbps DL) are primarily minimum design targets used to ensure overlap between cells is sufficient to maintain the minimum grade of service. Most user speeds will be significantly higher as user devices are likely distributed throughout a cell and speeds generally increase closer to the site as coverage increases (as depicted in Figure 2 Cell Edge Data Rate Design Targets). The Offeror should ensure that the peak/average network and user speeds are consistent with 3rd Generation Partnership Project (3GPP) standards for a 10x10 MHz LTE Frequency Division Duplex (FDD) channel and aligned with the 3GPP release feature set being deployed.

As part of the evaluation factors for award specified in Section M, each individual grid block will be assessed for meeting the definition of coverage. Only those grid blocks that have a reasonable amount of coverage will be considered acceptable. The Offeror should also maximize in-building coverage as

well as the amount of area and population covered that meets or exceeds the in-building link budget. The Offeror should use appropriate in-building penetration loss values for Band 14 and the various morphologies being considered.

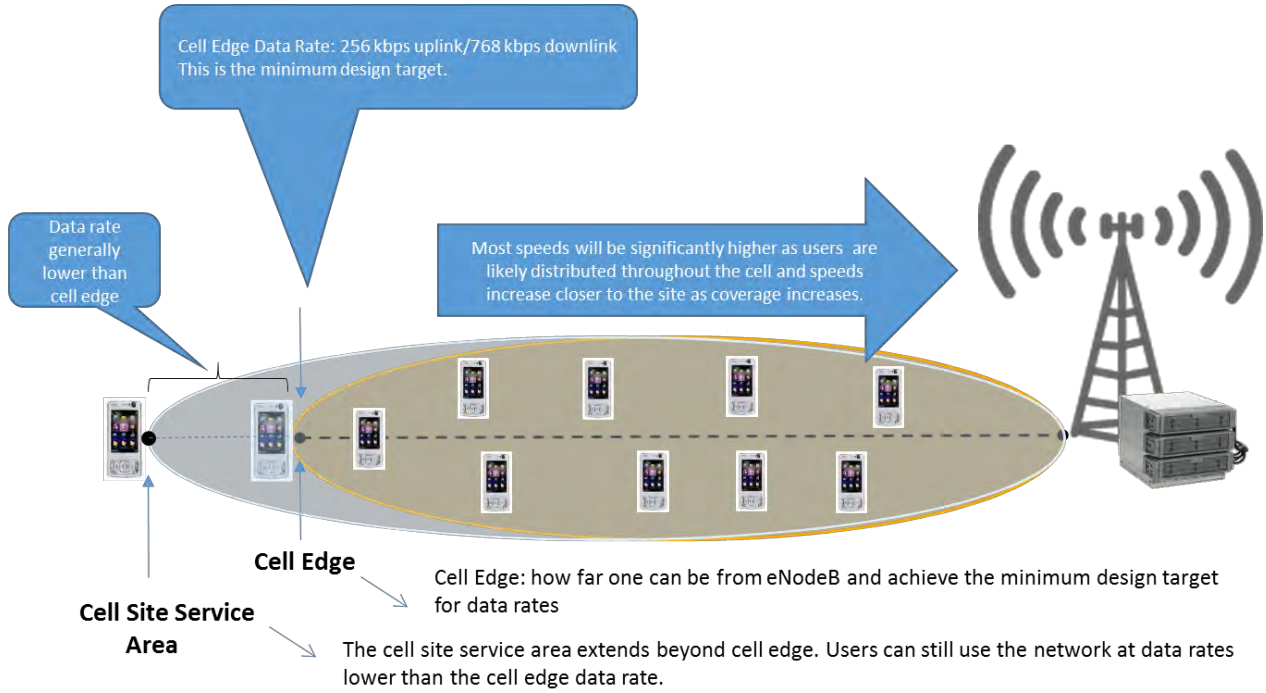


Figure 2 Cell Edge Data Rate Design Targets

3 Coverage Objective Map Methodology

The FirstNet baseline version of the coverage objective map was created from five distinct data sets and identifies areas that are likely to require a public safety response. This map was updated to incorporate state, territory, and tribal inputs, when available. FirstNet understands that a public safety response could be required anywhere. However, areas with a lower probability for a response would be identified as needing on-demand temporary or extended range coverage and capacity solutions.

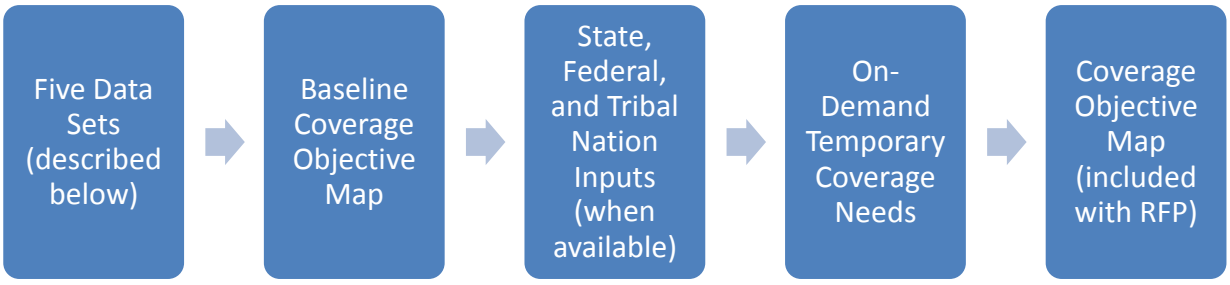


Figure 3 Baseline Coverage Objective Map Creation Methodology

The five data sets that were used to create the FirstNet baseline version of the coverage objective map are shown in Figure 4 Baseline Coverage Objective Map Data Sets. Each of the five data sets was combined into a single map and displayed in one-square-mile grid blocks.

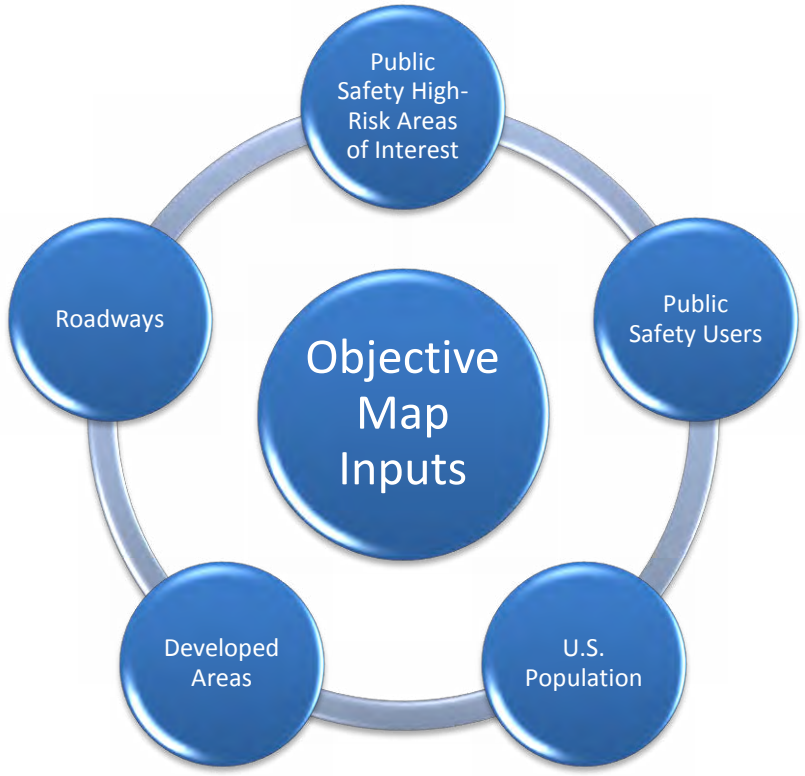


Figure 4 Baseline Coverage Objective Map Data Sets

3.1 Public Safety Users

This data set identifies the foundational user base for the network, which consists of law enforcement, fire, and emergency medical services users. The map distributes these users over their jurisdictional areas (i.e., city users are distributed throughout their respective cities, county users are distributed throughout their respective counties, and state users are distributed throughout their respective states).

3.2 Public Safety High-Risk Areas of Interest

This data set identifies key facilities, infrastructure, and locations that may be of particular interest to public safety users, such as public safety agencies, correctional facilities, airports, emergency operations centers, hospitals, schools, manufacturing facilities, energy plants, and large public venues.

3.3 U.S. Population

This data set identifies where people live using 2010 U.S. Census data.

3.4 Developed Areas

This data set helps determine response areas by identifying where people work as well as businesses and structures that may require response. The map includes areas classified as dense, medium, light, or open developed areas. This data can be found at http://www.mrlc.gov/nlcd11_data.php.

3.5 Roadways

This data set identifies commonly navigated roadways and significant secondary roadways using data from the National Highway System and annual average daily traffic counts.

4 Information for Coverage and Capacity Sub-Factor Evaluation

For the purpose of quantifying the coverage and capacity and rural coverage solutions specified in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, the Offeror should use the following data sets.

4.1 Population Map

FirstNet is providing a population map that contains the U.S. 2010 Census population data on a one-square-mile grid map (see Figure 5 Population Map). The population map, which covers each of the 56 states and territories, is included within Section J, Attachment J-1 as a shapefile (file titled "2010_Pop_Map_v1.0.mpk").

The Offeror shall provide population coverage maps in accordance with instructions in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.1.1.2, Non-Band 14 Population Coverage, and Section L.3.2.1.1.4, Band 14 Population Coverage.

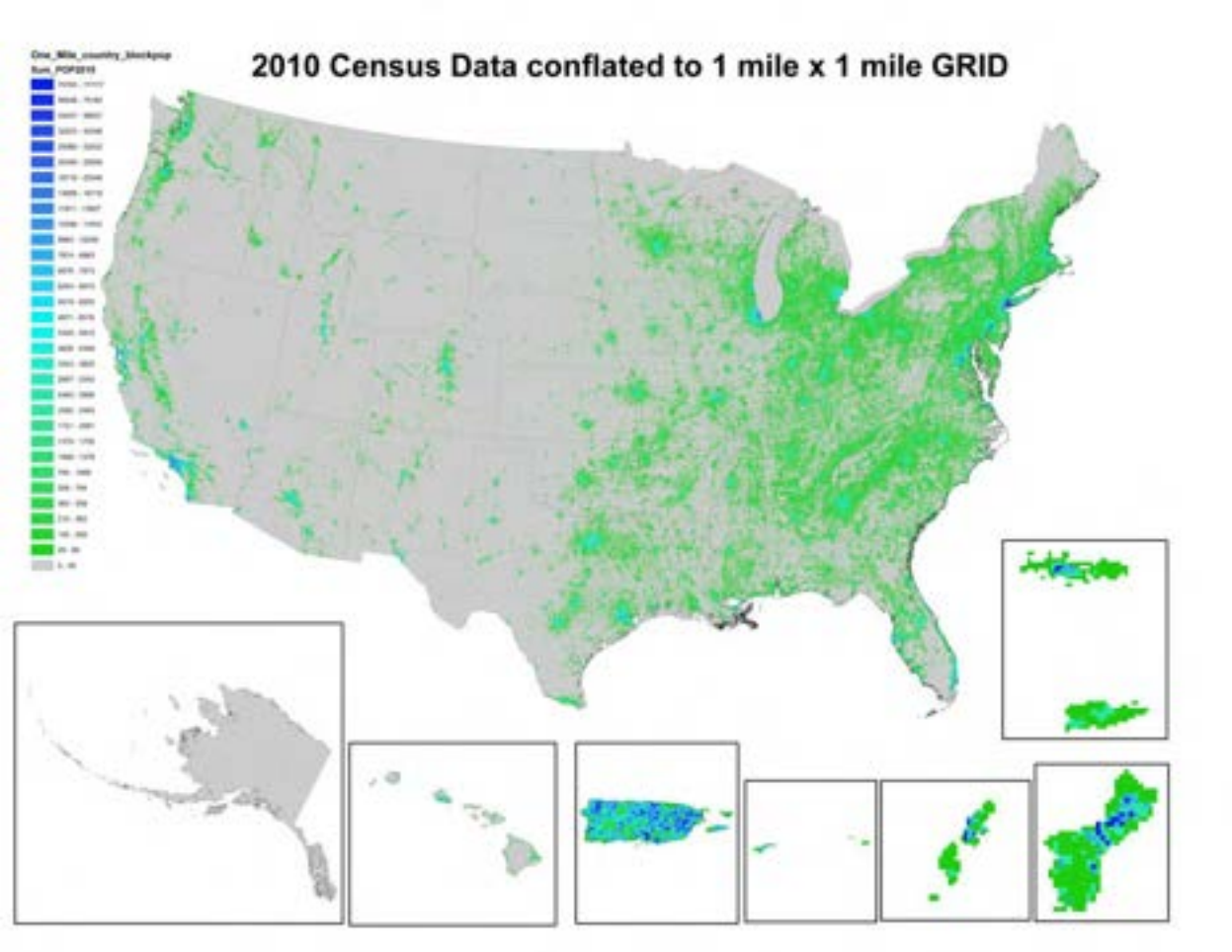


Figure 5 Population Map

4.2 Rural Definition Map

FirstNet is providing a rural definition map as shown in Figure 6 Rural Definition Map. See Section J, Attachment J-14, Terms of Reference, which summarizes the definition of "rural" found in the Rural Electrification Act of 1936. The rural definition map, which covers each of the 56 states and territories, is included within Section J, Attachment J-1 as a shapefile (file titled "Urban-Rural_Map_v1.0.mpk"). The Offeror should use this map to propose rural and non-rural coverage for the nation as a whole and for each of the 56 states and territories for the Initial Operational Capability (IOC)/Final Operational Capability (FOC)milestones, as explained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.1.3.2, Rural Coverage and Non-Rural Coverage.

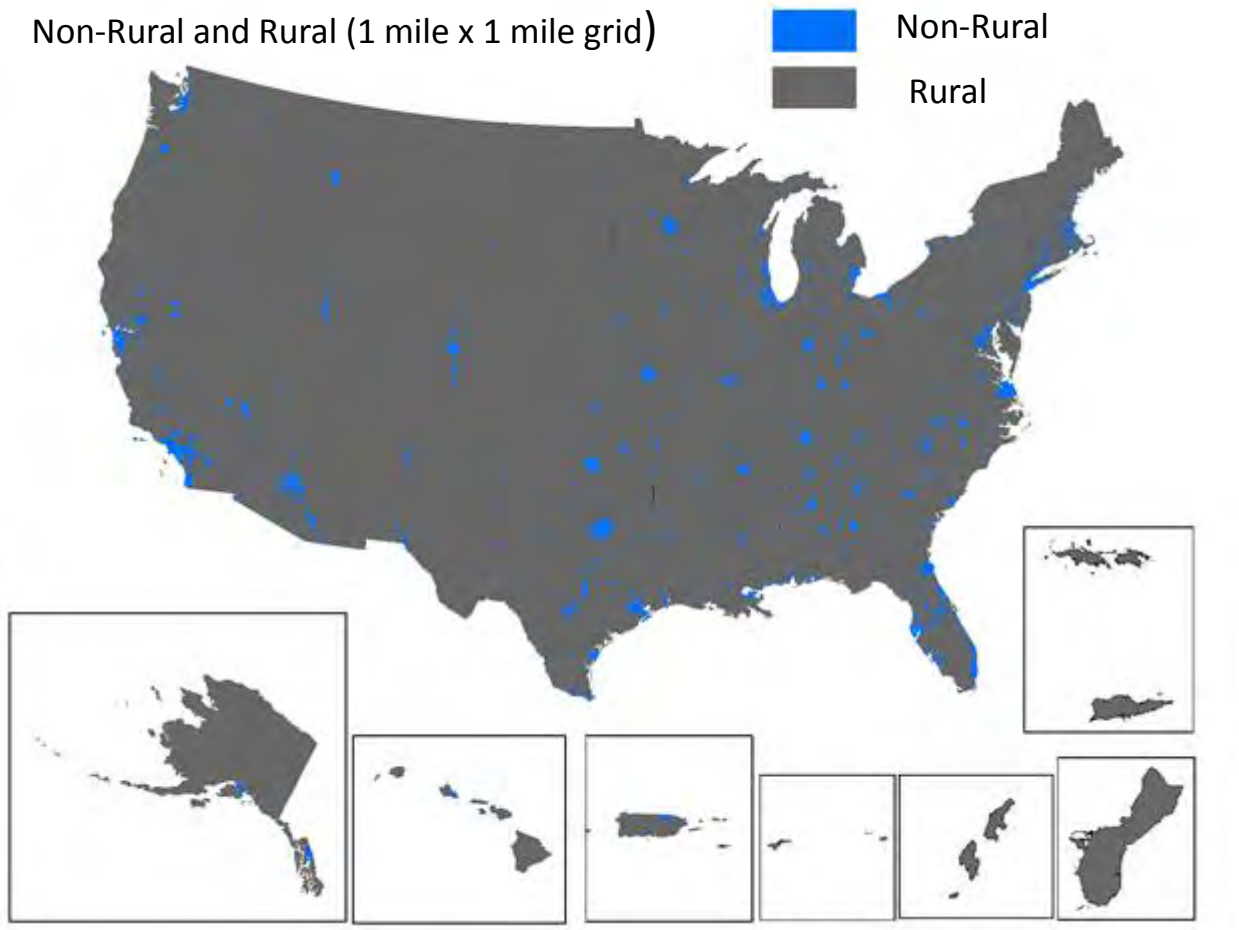


Figure 6 Rural Definition Map

4.3 Demand Map

FirstNet has aggregated stakeholder data to produce a nationwide view that estimates coverage demand at the county level. The demand maps include the number of devices used by those personnel, an estimate of eligible public safety users, and total monthly tonnage as of 2015. They can be seen in Figure 7 Heat Map by County/State/Territory – Device Density, Figure 8 Heat Map by County/State/Territory – Tonnage Density, and Figure 9 Heat Map by County/State/Territory – User Density. The maps were developed based on input from states, territories, tribal nations, and federal agencies, as well as FirstNet estimates. The demand maps are included within Section J, Attachment J-1 as shapefiles (files titled "Device_Demand_Map_v1.3.mpk," "Tonnage_Demand_Map_v1.3.mpk," and "User_Demand_Map_v1.3.mpk"), and as an Excel spreadsheet (file titled "Tonnage_User_Device_by_County.xls").

The Offeror should use these maps to quantify the Band 14 county-level capacity for each IOC and FOC milestone, as explained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.1.1.5, Band 14 Network Capacity.

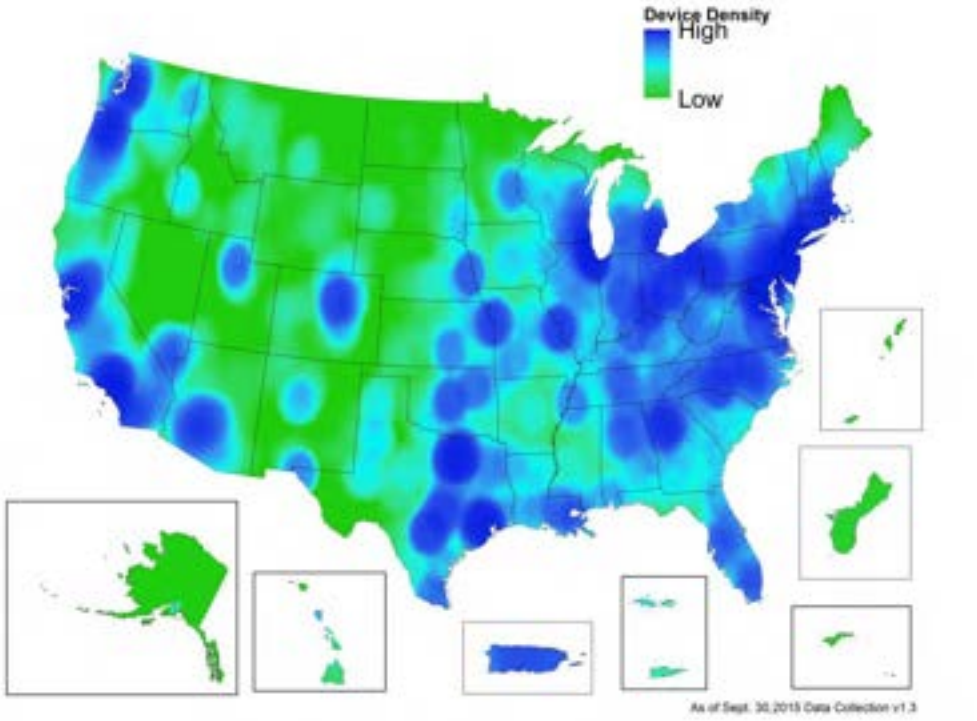


Figure 7 Heat Map by County/State/Territory – Device Density

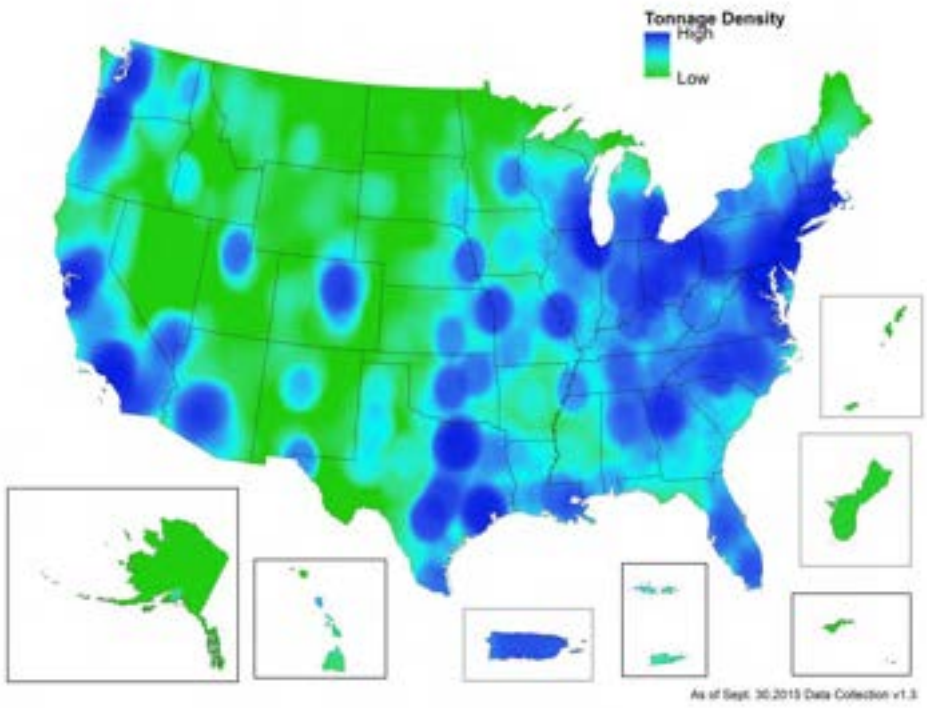


Figure 8 Heat Map by County/State/Territory – Tonnage Density

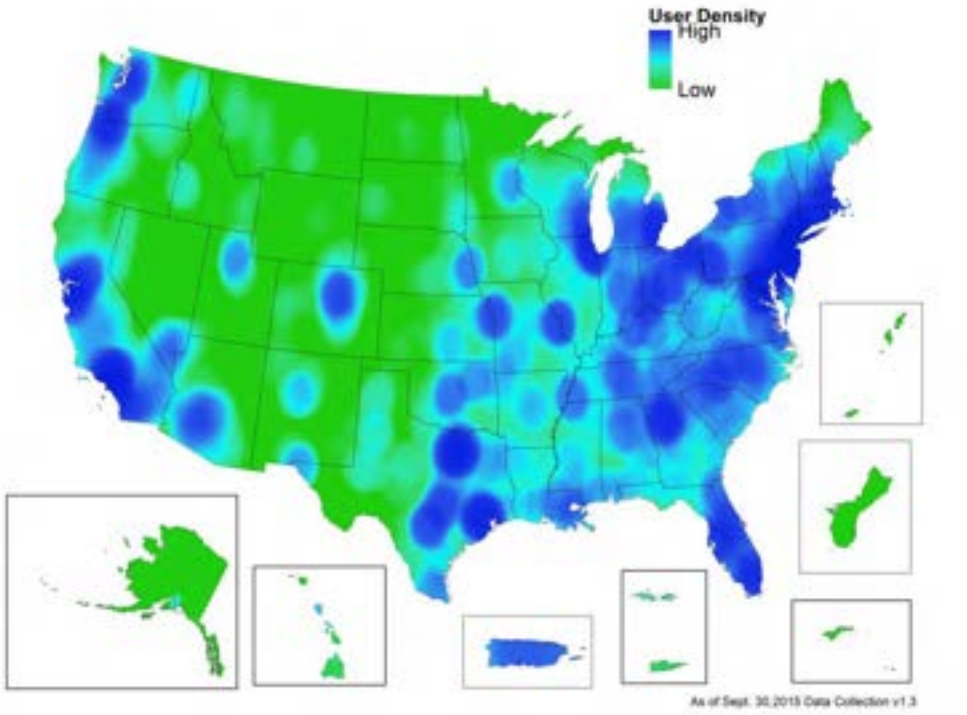


Figure 9 Heat Map by County/State/Territory – User Density

5 Definitions for LTE Analysis Layers

Below are the definitions of the LTE analysis layers requested in Section L, Instructions, Conditions, and Notices to Offerors or Respondents.

- **Reference Signal Received Power (RSRP)** – This layer provides the RSRP for the best carrier at each bin.
- **Best Server** – This layer provides the DL coverage area for the sector, which provides either the best RSRP or the best Reference Signal Received Quality (RSRQ) per the selection made in the network analysis options.
- **Downlink Signal-to-Interference-Plus-Noise Ratio (SINR)** – This layer provides the DL C/(N+I) or carrier to interference plus noise ratio (CINR) of the best carrier.
- **Uplink SINR** – This layer provides the UL C/(N+I) value of the best carrier.
- **Modulation and Coding Scheme (MCS)** – This layer provides information on the DL modulation that has the highest spectral efficiency (i.e., the modulation that provides the highest useful bits per symbol ratio) and where the coverage probability is above the defined target cell edge coverage probability.
- **Downlink Average Data Rate** – This layer provides the DL average data rate that could be achieved at any given location. It is the sum of the maximum data rate for all DL data paths, including all modulations present in a given location. Because the calculation of the layer includes all DL modulations, the layer may show higher values than the DL maximum achievable data rate layer.

- **Uplink Average Data Rate** – This layer provides the average UL data rate that could be achieved at any given location. It is the sum of the maximum data rate for all UL data paths, including all modulations present in a given location.
- **Composite Coverage Map** – This layer provides the extent of coverage. Where there is no coverage, the layer indicates whether the DL or the UL is the limiting factor.

Coverage Areas	Band 14		Non-Band 14		List of Rural Partners		Forecasted % of Rural Coverage Area Met through Rural Telecommunications Providers at FOC
56 States and Territories	Yes	No	Yes	No	Existing Partners	Planned Partners	
STATES							
Alabama							
Alaska							
Arizona							
Arkansas							
California							
Colorado							
Connecticut							
Delaware							
District of Columbia							
Florida							
Georgia							
Hawaii							
Idaho							
Illinois							
Indiana							
Iowa							
Kansas							
Kentucky							
Louisiana							
Maine							
Maryland							
Massachusetts							
Michigan							
Minnesota							
Mississippi							
Missouri							
Montana							
Nebraska							
Nevada							
New Hampshire							
New Jersey							
New Mexico							
New York							
North Carolina							
North Dakota							
Ohio							
Oklahoma							
Oregon							
Pennsylvania							
Rhode Island							
South Carolina							
South Dakota							
Tennessee							
Texas							

Coverage Areas	Band 14		Non-Band 14		List of Rural Partners		Forecasted % of Rural Coverage Area Met through Rural Telecommunications Providers at FOC
56 States and Territories	Yes	No	Yes	No	Existing Partners	Planned Partners	
Utah							
Vermont							
Virginia							
Washington							
West Virginia							
Wisconsin							
Wyoming							
TERRITORIES							
American Samoa							
Guam							
Northern Mariana Islands							
Puerto Rico							
U.S. Virgin Islands							

Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network

Prepared by:

Technical Advisory Board for First Responder Interoperability

Final Report

May 22, 2012

Contents

List of Tables

List of Figures

1 Executive Summary

1.1 Introduction

This report fulfills the statutory reporting requirements of the Technical Advisory Board for First Responder Interoperability pursuant to Title VI – "Public Safety Communications and Electromagnetic Spectrum Auctions" of the Middle Class Tax Relief and Job Creation Act of 2012 (Spectrum Act).[1] Pursuant to the Spectrum Act, the Federal Communications Commission (FCC) established the Technical Advisory Board for First Responder Interoperability (Interoperability Board). The duties of the Interoperability Board, in consultation with the NTIA, NIST, and the Office of Emergency Communications of the Department of Homeland Security, are twofold:

(A) Develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the Nationwide Public Safety Broadband Network (NPSBN); and
(B) Submit to the Commission [FCC] for review

In fulfillment of these duties, this report presents recommendations in the following areas:

- 3GPP LTE Standards, Interfaces and Guidelines
- User Equipment and Device Management
- Testing
- Evolution
- Handover and Mobility
- Grade of Service
- Prioritization and Quality of Service
- Security

1.2 Purpose

Across the United States, the public safety community responds to routine and emergency situations at a moment's notice regardless of the severity. These types of situations occur daily in every city and town in the country. The response of the public safety community relies on a communications network. Coordinated response, across agency lines, including multiple disciplines, is necessary to protect the communities and citizens the public safety community is charged to serve. In times of emergency, people look to their public safety officials to act swiftly and correctly, in order to do the things necessary to save lives, help the injured, and restore order. Most disasters will occur without warning. All require a rapid and flawless response. There is no room for error. Whether the event is a fire, natural disaster, vehicular collision, act of terrorism or the apprehension of a suspect, the key piece of that response is the ability to communicate. The communications network spans cities, counties and in some cases state borders. Without reliable and interoperable communications, the safety of our nation's first responders becomes jeopardized and the ability to perform their critical mission is compromised.

Two-Way Voice radio has been the predominant form of communication employed by public safety to date. With the advent of wireless broadband, we are at the beginning of the next major epoch in mission critical communication for first responders. The future wireless broadband network will offer additional data, video and voice services to further improve the effectiveness and safety of first responders. The report of the Interoperability Board specifies the "Minimum Technical Requirements" necessary to achieve a national interoperable broadband network for our nation's first responders. As specified in the Spectrum Act, FirstNet will use these recommendations to help develop and maintain the NPSBN, a goal which can only be met with through extensive and on-going cooperation among States and communities.

[1] Middle Class Tax Relief and Job Creation Act of 2012, Title VI – Public Safety Communications and Electromagnetic Spectrum Auctions.

This work is critically important to all first responders, and the future FirstNet organization that will develop, implement and manage the network. However, we must also remember that technologies are used by people. That component is the human factor. Whatever the technology, it will have to fit in the hands of those who will use it to protect and serve. It will have to be as simple to use as today‘s smart phones. It will have to be ruggedized and able to withstand the rigors of public safety use. The applications will need to be reliable and easy to use, whether a first responder is in pursuit of a subject, responding to a medical emergency, directing traffic or reporting to the scene of a disaster. The NPSBN will serve first responders who are part of the ―internet generation”. This generation of users grew up with mobile broadband technology; they adapt to it quickly and they understand the enormous capability that it affords. They aren‘t as concerned with who builds it as they are with what applications are available. Does it just work? Does it work everywhere? Is it automatic? What is the latest application that will assist me in my job? Will it be as reliable, resilient and predictable in times of emergency as the land mobile radio systems are today? Can I bet my life on it?

The underlying technology is one aspect of achieving interoperability; however, interoperability can only truly be established and preserved over time through vigilant policies, governance, and practices associated with creation, evolution and operation of the network by FirstNet.

1.3 Recommended Requirements Summary

In all cases where these recommendations reference specific 3GPP standards (e.g. 3GPP TS 36.101), the intended meaning is that the standard to be applied is contained in Release 9 of the 3GPP standards, or the future evolved equivalent of that standard that applies to future releases.

1.3.1 3GPP LTE Standards, Interfaces and Guidelines

[1] Hardware and software systems comprising the NPSBN SHALL implement interfaces consistent with Table 2: Standards Implementation Methodology.

[2] Hardware and software systems comprising the NPSBN SHALL support the interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

[3] Hardware and software systems comprising the NPSBN SHALL support management functions.

[4] Hardware and software systems comprising the NPSBN SHALL support APNs defined for PSAN usage.

[5] Hardware and software systems comprising the NPSBN SHALL support nationwide APNs for interoperability.

[6] Hardware and software systems comprising the NPSBN SHALL enable QoS control for PSAN-hosted applications via the 3GPP ‗Rx‘ interface.

[7] The NPSBN SHALL support IPv4, IPv6, and IPv4/v6 PDN types defined in 3GPP TS 23.401.

[8] The NPSBN SHALL support IPv4 and/or IPv6 transport for the EPS interfaces enumerated in Table 1: Minimum Interoperable Interfaces, consistent with the FirstNet design.

[9] Any sharing agreement that FirstNet enters into SHALL implement network sharing according to 3GPP TS 23.251 and SHALL NOT impact public safety operations.

[10] The NPSBN SHALL include the capability to collect and convey UE location data to applications using a standardized interface in near real time.

[11] The NPSBN SHALL be capable of providing public safety subscribers with access to the global Internet.

1.3.2 User Equipment and Device Management

[12] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP Release 9 Uu interface enumerated in Table 1: Minimum Interoperable Interfaces.

[13] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP TS 36.306 UE Radio Access Capabilities, Release 9.

[14] All User Devices (UEs) SHALL support interworking of the device with the USIM/USAT applications on the UICC in accordance with the relevant 3GPP 31.101, 31.102, and 31.111 standards.

[15] All User Devices (UEs) deployed on the NPSBN that support roaming onto commercial LTE networks SHALL operate on any FirstNet roaming partner network using bands supported by the device.

[16] All UEs SHALL support dual IPv4/IPv6 stacks.

1.3.3 Testing

[17] Prior to IOT and System-Level testing UEs SHALL have already met 3GPP conformance and certification requirements per an independent conformance testing organization (e.g. PTCRB).

[18] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required Interoperability Testing (e.g. using a subset of applicable test cases from CTIA IOT and UICC functional test cases, vendor IOT or similar commercial LTE industry practice).

[19] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required UICC functional testing.

[20] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interface Conformance Testing (e.g. testing S1-MME conformance to 3GPP) on the interfaces specified by FirstNet.

[21] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interoperability Testing at a system level as per the specific IOT requirements for the NPSBN.

[22] Infrastructure deployed on the NPSBN SHALL be included in the FirstNet-required FOA process as part of the NPSBN deployment.

1.3.4 Evolution

[23] The equipment comprising the NPSBN SHALL provide backwards compatibility of interfaces, from time of deprecation, for a minimum of two full major release/upgrades of the network. This requirement may be waived (i.e., interface obsolescence accelerated) if FirstNet can ascertain from the user community that there are no dependencies on a given interface.

1.3.5 Handover and Mobility

[24] The NPSBN SHALL support user mobility across the entire NPSBN (including Opt-out states).

[25] The NPSBN SHALL support S1 and SHALL preferentially support X2 handover between adjacent NPSBN cells (including cells owned by opt-out states) whose proximity supports a handover opportunity.

[26] If roaming between the NPSBN and commercial LTE networks is implemented, the NPSBN SHALL follow GSMA PRD IR.88.

[27] If roaming between the NPSBN and commercial 3GPP 2G/3G networks is implemented, the NPSBN SHALL follow 3GPP TS 23.002 to support roaming into 3GPP 2G/3G networks.

[28] If roaming between the NPSBN and commercial 3GPP2 (eHRPD) networks is implemented, the NPSBN SHALL follow 3GPP 23.402 to support roaming into 3GPP2 (eHRPD) networks.

[29] The NPSBN SHALL support the use of mobile VPN technology to support mobility between the NPSBN and other networks.

1.3.6 Prioritization and Quality of Service

[30] The NPSBN SHALL provide the ability for national, regional, and local applications to dynamically change a UE‘s prioritization and QoS using the 3GPP ‗Rx‘ interface.

[31] The NPSBN SHALL support all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.

[32] QoS mechanisms in the NPSBN SHALL comply with 3GPP TS 23.203.

[33] The NPSBN SHALL support the usage of all 15 ARP values defined in 3GPP 23.203.

[34] The NPSBN SHALL support the ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203.

[35] The NPSBN SHALL implement a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2.

[36] The NPSBN SHALL implement a nationwide scheme for assigning QoS Class Identifier priority to IP network and backhaul priority across the entire NPSBN.

[37] The NPSBN SHALL support the use of industry standard VPN and MVPN technology, while providing priority and Quality of Service for encapsulated applications.

1.3.7 Security

[38] The NPSBN SHALL use a nationwide common security profile for user plane and control plane traffic between UEs, eNBs and MMEs, in accordance with 3GPP LTE Network Access Domain protocols. The profile SHALL be based on 3GPP TS 33.401, and will be determined by FirstNet based on a system design and other considerations as it deals with evolving cyber threats. As a minimum, the profile SHALL include specification of ciphering algorithms (for example, use of AES-128 vs. SNOW 3G).

[39] The nationwide common security profile SHALL include ciphering of control plane traffic in order to provide for interoperable cyber protection of the network. Ciphering of user plane traffic is optional and is based on policy decisions that involve FirstNet and user agencies.

[40] To enable interoperable authentication, the USIM and HSS SHALL be capable of supporting the same key derivation functions, such as Milenage per 3GPP TS 35.205, 35.206.

[41] Network Domain Security SHALL be implemented in accordance with 3GPP TS 33.210, which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections

used to interconnect the domains).

[42] The NPSBN SHALL comply with TS 33.310 as the authentication framework for Public Key Infrastructure to authenticate these network interfaces.

[43] In order to ensure secure and interoperable interfaces between the NPSBN and external elements (e.g. all SGi, Rx and Srvs services as shown in Figure 2), these interfaces SHALL be protected with a FirstNet-approved security mechanism.

[44] User Domain Security SHALL be implemented in accordance with 3GPP TS 33.102, TS 31.101, and TS 22.022.

[45] USIM-based applications that require messaging between the USIM and network components SHALL implement Application Domain Security in accordance with 3GPP TS 33.102 and TS 31.111.

[46] In such cases where visibility is required for devices on the NPSBN, the implementations SHALL comply with 3GPP TS 33.102 and TS 22.101.

1.4 Recommended Considerations Summary

This section contains recommendations for consideration by the FCC and FirstNet as they develop finalized requirements to be included in RFPs. These recommendations for consideration are distinct from the recommended requirements in the previous sections, in that they are not considered by the Interoperability Board to be in scope as described in Section 3.2.

1.4.1 3GPP LTE Standards, Interfaces and Guidelines

(1) Hardware and software systems comprising the NPSBN SHOULD support integration of existing network elements via the necessary commercial standards-defined LTE interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

(2) Billing information from the NPSBN SHOULD be provided to each local and/or regional entity for the NPSBN services.

(3) The NPSBN SHOULD support existing Public Safety applications, deployed regionally or within agencies.

(4) The NPSBN SHOULD provide a method to connect a device to a packet data network where a ~~"h~~ome page" application is hosted with location specific content.

(5) The NPSBN SHOULD provide a method where a ~~"h~~ome page" application is available via an alternate access network, other than the NPSBN. This is a recommendation that the home page be made available and location-aware while roaming or over Wi-Fi.

(6) The NPSBN SHOULD provide a specification for locating a ~~"h~~ome page" based on current or manual location.

(7) The NPSBN SHOULD support use of field-deployed server applications.

(8) The NPSBN SHOULD support devices that are reachable via the global internet and can be used to host field based server applications (i.e. deployable servers).

(9) The NPSBN SHOULD allow the devices outside of their normal jurisdiction to connect to a local packet data network and to the device's home packet data network to carry out incident objectives.

(10) The NPSBN SHOULD provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages.

(11) Voice Sessions SHOULD be handed off within the NPSBN with limited delay and loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature is a future evolution capability.

(12) The NPSBN SHOULD support Voice over LTE (cellular voice) capabilities using GSMA PRD IR.92.

1.4.2 User Equipment and Device Management

(13) The NPSBN SHOULD allow the integration of high power LTE UEs as they become available, based on the methodology contained in Table 2: Standards Implementation Methodology.

(14) User Devices and Device Management solutions SHOULD support remote management capabilities over-the-air, including software update, discovery, device platform configuration, lock, unlock, wipe, and security configuration.

(15) The software systems that comprise the NPSBN SHOULD support the ability to enable local entities to install, update and manage their own applications. This may include security, transport and local APN provisioning.

(16) The software systems that comprise the NPSBN SHOULD provide published and version-controlled subscriber provisioning interfaces to enable end-to-end subscriber provisioning by the local entities. These interfaces SHOULD be verified during interoperability testing.

1.4.3 Testing

(17) Prior to operational deployment on the NPSBN, infrastructure equipment SHOULD have passed FirstNet-required Performance Testing of individual interfaces, nodes and overall system as per the specific performance requirements of the NPSBN.

(18) Nationwide applications on the NPSBN SHOULD have passed FirstNet-required security testing to proper security levels (e.g. Criminal Justice Information Services [CJIS]) to ensure protection of FirstNet and public safety information.

1.4.4 Evolution

(19) The NPSBN SHOULD allow for connection and operation of IP-based LMR voice interoperability gateways using open interfaces as they are developed.

(20) The NPSBN SHOULD be constructed and evolved in adherence to a multi-year roadmap.

(21) Infrastructure equipment procured for the NPSBN SHOULD support backwards compatibility with deployed LTE devices.

(22) Infrastructure equipment in the NPSBN SHOULD be upgradeable to minimally two major 3GPP releases (i.e. n+2, where n is the release available at deployment provided that the equipment does not need to implement a new air interface specification).

(23) Hardware and software systems comprising the NPSBN SHOULD support industry practices for management of standard network interfaces from each supplier. These industry practices include formal publication of interface compliance, deprecation of interfaces, support for backwards compatibility and graceful obsolescence of interfaces.

(24) The NPSBN SHOULD support industry practices for life cycle management of interfaces that it exposes to applications or users of the network to ensure backward compatibility for a reasonable interval, using industry-practice interface deprecation and obsolescence methods. The interfaces include, but may not be limited to: Network messaging Protocols, Application Programming Interfaces, Web-based Interfaces, Protocol/Messaging Interfaces, and User Interfaces such as Command Line Interfaces.

(25) The EPC equipment in the NPSBN SHOULD support optional local and geographic redundancy.

(26) The equipment in the NPSBN SHOULD support transport redundancy wherever economically feasible (i.e. connections to local switching equipment or WAN connectivity between sites or core locations).

1.4.5 Handover and Mobility

(27) If roaming between the NPSBN and commercial LTE networks is implemented, and IMS is implemented in the NPSBN, the NPSBN SHOULD implement support for IMS while roaming into other LTE PLMNs.

1.4.6 Grade of Service

(28) Coverage maps SHOULD be maintained that show pictorially which GoS Tiers are supported over a geographic area. Detailed maps SHOULD be made available to authorized public safety agencies.

(29) NPSBN coverage maps showing planned future coverage SHOULD be maintained. The maps SHOULD show planned coverage at regular intervals (e.g. quarterly) into the future. These maps SHOULD be made available to authorized public safety agencies.

(30) The NPSBN SHOULD use a set of pre-defined GoS Tiers to provide clear and uniform description of the services of network performance provided within a Coverage Area.

(31) The GoS Tiers SHOULD include the minimum set of GoS Attributes defined in Section 4.6.3.

(32) The expected or actual GoS Tier SHOULD be disclosed to authorized public safety agencies in a geographic region.

(33) Each Coverage Area SHOULD be designed to operate with a defined GoS tier.

(34) Service probability SHOULD be specified for each GoS Tier, in order to specify the quality of the user experience provided by the network.

(35) The expected minimum uplink (mobile to network) and downlink (network to mobile) rates of data transmission SHOULD be specified for each GoS Tier. The specifications must also include the protocol layer at which the data rates are to be measured.

(36) The NPSBN SHOULD implement a scheme for engineering RAN boundaries according to a national cell coordination plan.

1.4.7 Prioritization and Quality of Service

(37) A set of default QoS profile templates SHOULD be defined for each responder function (e.g. police, fire, EMS) supported by the NPSBN.

(38) Each QoS profile template SHOULD contain a descriptive definition of the responder function and default values for ARP, Access Class, UE-AMBR, and APN-AMBR.

(39) Since the NPSBN could also support secondary users, default QoS profile templates SHOULD be defined for public safety and secondary users.

(40) Every user of the NPSBN (public safety and secondary users) SHOULD be assigned a default prioritization and QoS profile using the set of pre-defined QoS profile templates.

(41) A process SHOULD be established and followed to manage the assignment of templates to users to ensure template assignment rules are uniformly applied for all users using the NPSBN.

(42) FirstNet SHOULD make an API available to national, regional, and local applications to expose Priority and QoS control.

1.4.8 Security

(43) The NPSBN security implementation SHOULD include pre-planned bypass mechanisms that have defined security and interoperability implications.

(44) Equipment used in the NPSBN SHOULD support AES and SNOW 3G algorithms.

(45) FirstNet SHOULD establish the security controls and policy for inter-domain security and require that all parties (e.g. public safety agencies) who connect to the NPSBN utilize FirstNet-approved cipher suites.

(46) FirstNet SHOULD consider using IPSec interfaces that utilize IKEv2 and utilize PKI to authenticate the peers of the IPSec Security Associations.

(47) When EPS elements are located in trusted locations without wide area communication links between them, the use of network domain security SHOULD be optional.

(48) Network interfaces between domains SHOULD be monitored and intrusion detection/prevention tools SHOULD be deployed.

(49) The developed security mechanisms SHOULD permit local entities to hide the topologies and address spaces of their networks.

(50) Security mechanisms layered by a jurisdiction on top of the NPSBN SHOULD NOT inhibit interoperability for users visiting from outside of the security domain in which it is implemented.

(51) As FirstNet enters into roaming agreements with commercial partners, security policies SHOULD be implemented that ensure integrity of the NPSBN and that NPSBN security practices are not compromised.

(52) FirstNet SHOULD consider supporting implementation of a national framework for user identity management.

(53) FirstNet SHOULD consider supporting implementation of a national framework for user identity federation to enable user interoperability across administrative domains within the NPSBN, where authorized.

(54) Implementation of the national framework for user identity management and federation SHOULD include

a set of guidelines and rules for applications to participate in the national identity management framework.

(55) The agency, organization or entity that utilizes the NPSBN Identity Management framework SHOULD be responsible for enforcing authorization constraints on access to information as per their own security policy.

2 Introduction

2.1 Statutory Framework for Deployment of a Nationwide Interoperable Public Safety Broadband Network

The Spectrum Act established the First Responder Network Authority (―FirstNet") as ―an independent authority within [the National Telecommunications and Information Administration (NTIA)]"[2] to ―ensure the establishment of a nationwide, interoperable public safety broadband network."[3] FirstNet is also the spectrum licensee for the re-allocated D Block for public safety services and the existing public safety broadband spectrum, collectively referred to as Band 14.[4]

Under the Spectrum Act, the FCC was responsible for selecting the membership of the Technical Advisory Board for First Responder Interoperability (Interoperability Board),[5] which was tasked to develop recommended ―minimum technical requirements for interoperability"[6] for the FCC to submit to the FirstNet (with possible revisions). The Interoperability Board will ―terminate 15 days after the date on which the Commission transmits the recommendations to the First Responder Network Authority".[7]

FirstNet will then use the minimum technical requirements for interoperability to develop and issue RFPs for the construction and operation of the NPSBN, ―without materially changing them." FirstNet has been funded up to $7 Billion from incentive auctions to be deposited in a Network Construction Fund. To pay for operating expenses, FirstNet is authorized to assess user fees and fees associated with leasing network capacity and infrastructure.

The Spectrum Act also provides a process by which a State may choose to ―Opt Out" of the planned FirstNet deployment in its jurisdiction and operate its own radio access network. As a component of this process the FCC will evaluate the State's alternative plan using the minimum technical requirements for interoperability as a component of its evaluation. The FCC will determine whether the State's plan or the FirstNet plan will be used for the construction and operation of the radio access network (RAN) network within the State. States that successfully opt out must be interoperable with the NPSBN.

2.2 Technical Advisory Board for First Responder Interoperability

The Spectrum Act required that the FCC Chairman establish the Interoperability Board within 30 days of

---

[2] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6204 (a).

[3] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6202 (a).

[4] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6201(a).

[5] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (a).

[6] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1).

[7] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (f).

enactment. The Interoperability Board is required to consist of 15 members, with 14 voting members appointed by the FCC and one non-voting member appointed by the National Telecommunications and Information Agency (NTIA). The Spectrum Act requires the Interoperability Board membership to be made up of 4 representatives of wireless providers; 3 representatives of equipment vendors; 4 representatives of public safety entities; 3 representatives of State and local governments; and one non-voting member appointed by NTIA.

The FCC issued a Public Notice on February 28, 2012 seeking nominations to the Technical Advisory Board. [8] FCC Chairman Julius Genachowski appointed the fourteen voting members of the Technical Advisory Board for First Responder Interoperability (Interoperability Board) on March 22, 2012.[9] Those selected for membership on the Interoperability Board are identified in Section 2.2.1 below.

The Interoperability Board held its initial meeting on March 23, 2012 to begin developing its structure and processes for accomplishing its legislative mandate.[10] In this meeting the Chairman (Charles L. K. Robinson) and Vice Chairman (Kenneth C. Budka) were elected by the board members and the board established the agenda for its second meeting, which was a face-to-face meeting held on March 26 and 27, 2012.

This second meeting of the Interoperability Board focused on developing a mutual understanding of the general definition of interoperability, the scope of topics necessary to ―ensure a nationwide level of interoperability"[11], how the Interoperability Board should structure itself to accomplish this work, and a schedule to meet the statutory deadline for completing the work.[12] After developing consensus around the general elements of the definition of interoperability, the Interoperability Board developed a scope for its work, organized itself into four subcommittees, and selected Chairpersons for each subcommittee.

- Subcommittee 1 focused on Standards, Interfaces, and Guidelines; User Equipment and Device Management; and Network Evolution; (Chair: Paul Steinberg)
- Subcommittee 2 focused on Mobility and Handover; Grade of Service; Prioritization and Quality of Service; (Chair: Kenneth C. Budka)
- Subcommittee 3 focused on Security; (Chair: Brian Shepherd) and
- Subcommittee 4 served as the Drafting Subcommittee (Chair: Dennis Martinez) and was responsible for organizing the content of the Interoperability Board's report.

The Interoperability Board adopted the principle of transparency as a key component of its work and success. This principle guided the board's discussion on how best to engage the public and meet its statutory requirement to consult with the National Telecommunications and Information Agency (NTIA), the National Institute of Standards and Technology (NIST), and the Office of Emergency Communications (OEC) of the Department of Homeland Security[13] - hereafter referred to as ―Consulting Agencies". During its March 26th session, the Interoperability

[8] Federal Communications Commission Public Notice DA 12-303.

[9] Federal Communications Commission Public Notice DA 12-455.

[10] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c).

[11] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1)(A).

[12] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1).

[13] Middle Class Tax Relief and Job Creation Act of 2012, Title VI (Public Safety Communications and Electromagnetic Spectrum Auctions), Section 6203 (Public Safety Interoperability Board), (c)(1).

Board decided that beginning with its session on March 27th the Consulting Agencies would be allowed to listen in or be present at all open Board meetings. Although the Consulting Agencies could not participate in the board's deliberations, they were able to respond to questions and provide documentation if requested by the board. The board did have several closed sessions for deliberations at which no one except board members were present.

The Interoperability Board was also keenly aware of the interest in, investment in, and commitment to the success of the NPSBN by organizations and individuals outside of the board's membership and the Consulting Agencies. The Interoperability Board took action at its March 26th session to ensure that these organizations and individuals could participate in the development of its recommendations in two ways: the Interoperability Board requested that the FCC open a docket[14] to receive input from interested parties and established a date to conduct a Public Workshop[15] to seek information from the public on the components of interoperability the board considered within its scope.

While the members of the Interoperability Board were leaders in their organizations and individual areas of expertise, the board quickly realized that they would need the help of subject matter experts (SMEs) - both inside and outside their organizations in order to complete work within the statutory time limit. At its March 27th session, the board developed rules for the engagement of SMEs in its work processes. This engagement proved to be critical to the quality of the board's work and to the overall success of the board.

The Interoperability Board developed a timeline for completing its work, completed the organization of the subcommittees and held the initial meetings of its subcommittees on March 27th. The board closed this second meeting by establishing the preliminary schedule for subcommittee meetings. Over the next three weeks, subcommittees conducted individual conference calls up to three times per week with a goal of having an initial draft of their recommended requirements by April 19, 2012. Many board members participated in subcommittee conference calls outside of their assigned subcommittee, devoting much of their available time to this important work. The Chairman of the Drafting Subcommittee developed a document framework for the board's final report and each subcommittee began developing their recommended requirements according to this framework.

The Interoperability Board conducted its Public Workshop on April 23, 2012. The workshop consisted of four panels with four speakers on each panel. Speakers were selected to provide the board with the broadest perspectives possible on the issue of interoperability within the NPSBN[16]. After the Public Workshop, the board held work sessions on April 23rd and 24th. On April 23rd, subcommittees met to consider the information they had received in the Public Workshop. On April 24th, subcommittees briefed the board on their initial recommended requirements and how the information received at the Public Workshop would impact their work.

On April 23rd, the board decided how to proceed with its statutory consultation requirement with the Consulting Agencies. The board decided to provide the Consulting Agencies with its draft recommendations document on April 27, 2012 and request that the Consulting Agencies provide any suggested changes, comments, and recommendations by May 2, 2012. The board also elected to provide the FCC with the same opportunity. In addition to having the opportunity to provide specific suggested changes, comments and recommendations on the draft document, each of the Consulting Agencies and the FCC were invited to participate in the board's May 2nd conference call to provide a summary and context for their recommendations.

In closing its work session on April 24, 2012, the Interoperability Board decided to no longer meet as subcommittees after April 27th. Subcommittees would work to incorporate the germane information they received during the Public Workshop and provide it to the Drafting Subcommittee Chairman by April 27, 2012. Beginning on April 30th, the Interoperability Board met three days a week to continue refining its recommended requirements

[14] Federal Communications Commission Public Notice DA 12-474

[15] Federal Communications Commission Public Notice DA 12-538 and 12-617

[16] Federal Communications Commission Public Notice DA 12-617

through May 14, 2012. The board also set the date for its final work session at the FCC offices on May 16th and 17th.

The May 2nd meeting between the Interoperability Board, the Consulting Agencies and the FCC proved to be invaluable in developing the recommended requirements. The suggested changes, comments and recommendations to the draft document were thoughtful, forward thinking, and focused on the board's statutory responsibilities. The summary and contextual comments provided during the meeting effectively framed their suggestions for the document and provided the board a better understanding of the context of their recommendations.

The Interoperability Board continued to refine its recommended requirements leading up to its work session on May 16 and 17, 2012. As the work continued the defined scope became more precise and the number of requirements began to drop. For example, from Version 1.1 of the board's recommended requirements to Version 1.2, there was a 30% reduction in the number of recommended requirements.

As the Interoperability Board met for its final scheduled work session on May 16th and 17th, its members were confident in the board's ability to meet the target completion date. Though much had been accomplished over the previous 7 weeks, the open issues proved to be the most difficult for the board to resolve. Over these two days the board continued the process of open collaboration between its members, their SMEs and the Consulting Agencies that had brought it successfully to this final session. In the end these difficult issues were resolved with the same focus and commitment the board had demonstrated throughout its work.

As demonstrated here, the Interoperability Board organized itself quickly, developed an effective execution plan, and diligently worked this plan to meet the statutory mandate. In the process, the board not only included the Consulting Agencies as required by statute, but provided ways for other organizations and individuals to participate. The board's commitment to transparency and seeking the broadest possible input within its constrained schedule has resulted in a set of recommended minimum technical requirements, within the scope of the Spectrum Act, that will ~~–~~ensure a nationwide level of interoperability".

2.2.1 Interoperability Board Membership

The Interoperability Board was comprised of the following members:

- Bob Azzi, Senior Vice President, Network, Sprint Nextel Corporation
- Todd Bianchi, Firefighter Paramedic, Washington, District of Columbia Fire and EMS Department
- Kenneth C. Budka, Senior Director, Advanced Mission-Critical Communications, Bell Labs Chief Technology Office, Alcatel-Lucent
- Ed Chao, Senior Vice President, Corporate Engineering and Network Operations, MetroPCS Communications, Inc.
- Brenda L. Decker, Chief Information Officer, State of Nebraska
- Colonel Kenneth C. Hughes, Jr., (Ret), Regional Communications Coordinator, New Orleans Urban Area Security Initiative
- Dennis Martinez, Chief Technology Officer, RF Communications Division, Harris Corporation
- Dereck Orr, Program Manager, Public Safety Communications Standards, Office of Law Enforcement Standards, NIST (non-voting member representing NTIA).
- Bill Price, Director Broadband Programs, Department of Management Services Division of Telecommunications, State of Florida
- Steve Proctor, Executive Director, Utah Communications Agency Network
- Charles L. K. Robinson, Director, Business Support Services, City of Charlotte, North Carolina
- Brian Shepherd, Deputy Director, Adams County (Colorado) Communication Center
- Paul Steinberg, Senior Vice President and Chief Technology Officer, Motorola Solutions, Inc.
- Ron Strecker, Chief Executive Officer, Panhandle Telephone Cooperative, Inc., and Panhandle Telecommunications Systems, Inc.
- Diane C. Wesche, Executive Director, Government Network & Technology, Verizon

3 Objective, Scope, and Methodology

3.1 Objective

The adoption of LTE technology will fundamentally change the way first responders communicate. Additionally, the establishment of FirstNet will fundamentally change the ways public safety networks are built, operated and maintained.

Adoption of LTE technology, a technology embraced by commercial service providers worldwide will bring significant benefits to first responders. Adoption of LTE makes the NPSBN part of a multi-billion dollar commercial technology ecosystem, allowing first responders to take advantage of current and future advances in wireless communications technology, wireless devices, applications, networking, security and network infrastructure. Further, adoption of LTE allows public safety to benefit from the exceptionally high level of interoperability achieved on commercial service provider networks.

The high level of interoperability achieved on commercial service provider networks did not happen by accident. One critical factor responsible for the high level of interoperability achieved on commercial service provider networks is the process used by the commercial market to develop and maintain technology standards. The open, consensus-based process adopted by 3GPP, for example, creates a forum which encourages both technological innovation and the maintenance of backward compatibility. This approach has allowed service providers to offer new services while protecting the significant investments they have made in the construction and operations of their networks.

The use of rigorously defined architectures and interfaces in LTE promotes interoperability by giving service providers stable interfaces around which to design their networks. Furthermore, this practice promotes competition, drives innovation and lowers costs among vendors of equipment, user devices, software and services.

One of the most significant factors responsible for the high level of interoperability achieved on commercial service provider networks is the *extensive* testing that is performed to ensure adherence to standards and inter-vendor interoperability.

While public safety communication requirements share a tremendous amount of commonality with the communications requirements of the consumer market, there are notable differences. We expect that many of these requirements can be satisfied with standard interfaces and features supported (or planned to be supported) by LTE. In some cases, FirstNet may opt to implement functionality either not supported by LTE standards or LTE features not in use by commercial service providers. The rewards of such functionality must be carefully weighed against the risks of maintaining interoperability as LTE evolves and the potential high costs incurred through such customization.

Under the Spectrum Act, the Interoperability Board is required to ~~"d~~evelop recommended minimum technical requirements to ensure a nationwide level of interoperability for the nationwide public safety broadband network." The Spectrum Act further requires the Interoperability Board to ~~"b~~ase the recommended minimum technical requirements on the commercial standards for Long Term Evolution (LTE) service."

In developing the minimum technical requirements contained in this document, the Interoperability Board's objective has been (1) to create in the NPSBN levels of interoperability that mirror the levels of interoperability achieved in commercial service provider networks and (2) to reflect how LTE technology would be used to meet public safety's unique mission requirements. In doing so, we have been guided by a foundational philosophy: in order for the NPSBN to take advantage of the interoperability achieved by LTE, FirstNet must *fully* embrace the technologies, standards and best practices used by commercial service providers to ensure interoperability on day 1 of network deployment and beyond.

3.2 Scope

The U.S. Department of Homeland Security's SAFECOM program's Interoperability Continuum[17] establishes the critical elements that must be addressed to ensure communications interoperability. These elements include governance, standard operating procedures, technology, training and exercises, and usage of interoperable communications. It is important to note that technology - the focus of the Interoperability Board as mandated by the Spectrum Act - is but one aspect of the work needed to ensure a nationwide level of interoperability for the NPSBN. Furthermore, since LTE is but one of the many technologies that will be deployed in the NPSBN, development of technical requirements for LTE is but part of the work needed to address the technology elements of interoperability.

The U.S. Department of Homeland Security's SAFECOM program defines interoperability as ~~–~~the ability of emergency response agencies to talk to one another via radio communications systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized."[18] SAFECOM's definition of interoperability covers the full spectrum of public safety communications. Because of the Interoperability Board's focus on minimum technical interoperability requirements based on commercial standards for Long Term Evolution (LTE) technology, the Interoperability Board felt it prudent to adopt a definition of interoperability that more appropriately reflected this limited scope.

The success of meeting the goal of a nationwide level of interoperability for the NPSBN will be grounded in the actions taken by the Interoperability Board in setting technical requirements that will allow for the deployment of a network comprised of equipment, services, and applications from a diverse set of companies.

For the purpose of facilitating the Interoperability Board's work under the limitations placed upon it by the Spectrum Act of 2012, we define ***interoperability*** as the ability of all authorized local, state and federal public safety entities and users to operate on the NPSBN and commercial partner networks, to access rapid, reliable and secure communication services, in order to communicate and share information via voice and data. These communications services must support existing and future applications and operate across functional, geographic and jurisdictional boundaries.

We note that the NPSBN will be implemented in phases using equipment from multiple vendors. It is therefore important to ensure interoperability is maintained throughout all deployment phases. As discussed in Section 4.6.4, for example, we note that careful planning is required to ensure seamless service across potential implementation boundaries that may be introduced during the build out of the NPSBN's RAN. Such implementation boundaries, for example, can exist between eNBs provided by different vendors or between RAN segments deployed and managed by states which have decided to exercise the Spectrum Act's opt out provision.

The scope of the Interoperability Board's requirements is limited to minimum requirements necessary to facilitate ***technical interoperability*** in the NPSBN. Technical interoperability is defined as follows:

> ***Technical interoperability is the ability of two or more systems or components, from the same or different manufacturers or service providers, to successfully exchange data and use information based on underlying interface standards.***

It is important to note that this derived scope eliminates governance, operational, policy and procedural practices from our consideration in developing recommended minimum technical requirements. However, in cases where deemed important, the Interoperability Board did include ***Recommended Considerations*** covering subject matter outside of this derived scope.

---

[17] See http://www.safecomprogram.gov/SiteCollectionDocuments/Interoperability_Continuum_Brochure_2.pdf

[18] http://www.safecomprogram.gov/about/default.aspx.

In finalizing its set of recommended requirements, the Interoperability Board carefully assessed the sometimes competing factors. There were many discussions around the following topics:

- Whether draft requirements could be considered ―minimum technical requirements" as mandated by the Spectrum Act
- Whether draft requirements addressed operability or interoperability
- Whether draft requirements were technical or operational
- Striking a proper balance between granting FirstNet the flexibility it will need to build and maintain the NPSBN while providing the specificity needed to both set a proper course for FirstNet and give the FCC useful tools to determine whether to approve State opt-out plans
- The proper of level of detail to specify requirements in the absence of a nationwide network architecture
- How best to ensure interoperability is maintained as FirstNet and LTE technology evolves

3.3 Methodology

3.3.1 Assumptions

The Interoperability Board made two key assumptions in developing its recommendations:

- The Interoperability Board could not assume any particular network architecture.
- The requirements would use 3GPP LTE Release 9 as the baseline reference point.

The first assumption was made to ensure that the final architecture of the NPSBN was reflective of FirstNet's deployment plans. Accordingly, the board's recommendations reflect the possibility that the NPSBN could consist of either a homogenous or heterogeneous network architecture. The board's assumption of the possibility for a heterogeneous network architecture was based on the Spectrum Act's requirement for FirstNet to leverage interim existing federal, state, tribal, and local infrastructure ~~to~~ the maximum extent economically desirable".[19]

3.3.2 Public Safety Requirements and LTE Standards

Public safety imposes unique requirements that cannot all be satisfied with LTE standards that are available today. This is represented in Figure 1 below. An example of such a requirement is Mission Critical Voice, which includes Push to Talk (PTT), off-network operation, and a variety of related functions.

Therefore, as LTE standards continue to evolve, and organizations such as FirstNet participate in the 3GPP standards processes to drive desired capabilities, more of the public safety requirements can be satisfied with products based on these standards.

[19] Middle Class Tax Relief and Job Creation Act of 2012, Title VI, Section 6206, (c)(3).

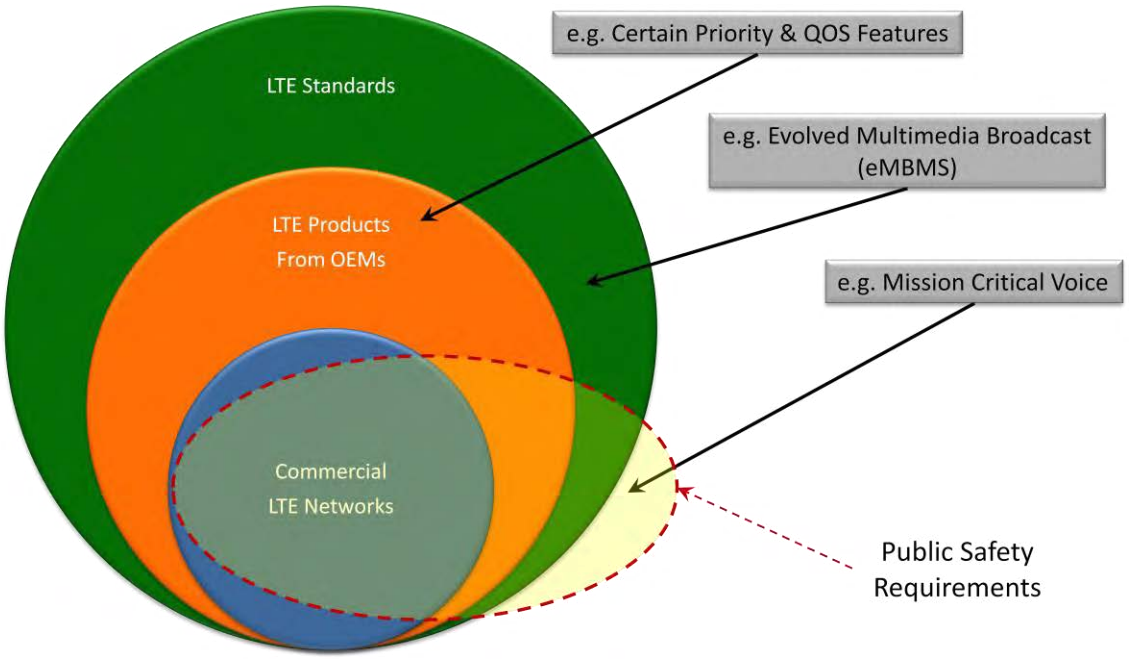


Figure 1: Public Safety Requirements and Standards

3.3.3 Document Structure

Section 4 of this report contains the Interoperability Board's recommendations for minimum technical requirements to ensure a nationwide level of interoperability for the NPSBN. The structure of the recommendations is consistent with common practice for development of technical requirements that are part of an RFP process, with some noteworthy explanations.

Recommended requirements are explicitly noted in the document and use the exclusive verb forms SHALL and SHALL NOT. These are referred to as *Normative* clauses. Recommended requirements are very short, usually single sentences per requirement. Many recommended requirements require a contextual framework to ensure that the requirement is interpreted in an unambiguous way. Therefore the document contains *Informative* language that frames the recommended requirements in their proper context, and therefore *Informative* clauses should accompany the requirements in RFPs.

The document also contains recommendations for consideration that are not phrased as *Normative* clauses. These recommendations for consideration are generally noted explicitly and/or use verb forms such as SHOULD and SHOULD NOT. The Interoperability Board included these types of recommendations to indicate that the subject matter should be addressed by FirstNet as it carries out its duties under the Spectrum Act, but these recommendations fall outside the Interoperability Board's scope, as described in Section 3.2.

4 Recommendations

In this section, the Interoperability Board details its recommended minimum technical requirements to ensure a nationwide level of interoperability. In addition it details recommended considerations that lie outside the scope of these recommended minimum technical requirements. The latter are provided as recommendations that FirstNet should consider as it develops more complete requirements as part of its RFP processes.

In all cases where these recommendations reference specific 3GPP standards (e.g. 3GPP TS 36.101), the intended meaning is that the standard to be applied is contained in Release 9 of the 3GPP standards, or the future evolved equivalent of that standard that applies to future releases.

4.1 3GPP LTE Standards, Interfaces and Guidelines

The Spectrum Act requires the Interoperability Board to develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the NPSBN. The Spectrum Act provides that these recommendations shall be based on the commercial standards for LTE technology. LTE is a common term used to describe a family of global standards that are specified by the Third Generation Partnership Project (3GPP). LTE is an all-Internet Protocol technology platform that is composed of a set of network elements within the 3GPP network architecture. These network elements constitute the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and associated Evolved Packet Core (EPC) and support other network elements. The E-UTRAN and EPC are collectively referred to as the Evolved Packet System (EPS).

3GPP specifications, the LTE specifications in particular, are broad in the scope of functionalities that they address. Only a minimum subset of these specifications are required for the NPSBN to be interoperable nationwide. Specification of a 3GPP standards release does not necessarily guarantee that implementers will build products supporting all the features appearing in the release. Implementing a feature typically requires support across the LTE ecosystem: service providers, chipset manufacturers, user device manufacturers, network infrastructure manufacturers, software developers, etc. Market needs that were anticipated when planning for a release may have changed by the time implementation negotiations begin. As a result, only a subset of the features in each release will typically initially be implemented. Additional features may be phased in at a later stage or may never be developed. This dynamic has important implications for planning the evolution of the NPSBN. Each LTE release provides additional functionality that may be beneficial to public safety. Evolution plans must take into account the features planned for each LTE release as well as what actually gets implemented commercially (and also specific vendor availability). In addition, specific features required by public safety may not be supported by the commercial requirements driving LTE standards. In these cases, either alternative ways must be found to realize the desired functionality or new functionality must be introduced into the 3GPP standards.

Furthermore, there are specifications and guidelines developed by other bodies such as the GSM Association (GSMA) and the Open Mobile Alliance (OMA) that warranted consideration as minimum technical requirements in order to enable the interoperability of the NPSBN. These factors were examined in the process of identifying the minimum technical interoperability requirements for the network, recognizing that interoperability problems can occur if network requirements are ambiguous or not defined with sufficient specificity.

The minimum technical requirements recommended to FirstNet are an input to the RFPs to be issued by FirstNet for vendor bids and contracts. The RFPs issued by nationwide wireless service providers and the resulting contracts typically make extensive use of references to the technical specifications that are developed by bodies such as 3GPP. The Interoperability Board anticipates the same will hold true for FirstNet. Because the minimum technical requirements developed by the Interoperability Board will be used by FirstNet in developing RFPs, the minimum requirements that the Interoperability Board developed include specific reference to 3GPP technical specifications, interfaces, and options within the standard. These specifications, accompanied by a rigorous testing regimen, can ensure that the products from multiple vendors, and the interworking of network elements across multiple jurisdictions by a diverse community of users, are interoperable. Considering a minimum subset of LTE specifications in the RFP process is important to ensure the nationwide interoperability of the NPSBN.

4.1.1 Interoperability Assumptions

The following assumptions are reflected throughout Section 4.1:

1. The NPSBN EPC elements will use a single common PLMN ID for supporting public safety users. If the NPSBN RAN is shared with other EPCs, on a secondary basis, those EPC elements will use one or more PLMN IDs which are different from the NPSBN PLMN ID used for public safety users.
2. The interoperable EPC functions and interfaces are expected to be based on 3GPP Release 9 or later.

Given that technology evolves rapidly, the network components and associated interfaces identified in the present document are also expected to evolve over time. As such, these aspects of the present document are intended to represent a state-of-the-art snapshot at the time of writing. In this context, the standards, functions, and interfaces referenced in the present document are intended to prescribe statements of intent. Variations or substitutions are expected to accommodate technological evolution consistent with the evolution of 3GPP and other applicable standards.

4.1.2 NPSBN Landscape Diagram

The following diagram is a top-level „landscape‘ view of the networks associated with the NPSBN. The specific networks which are in-scope of the present document are encapsulated in the dashed box.

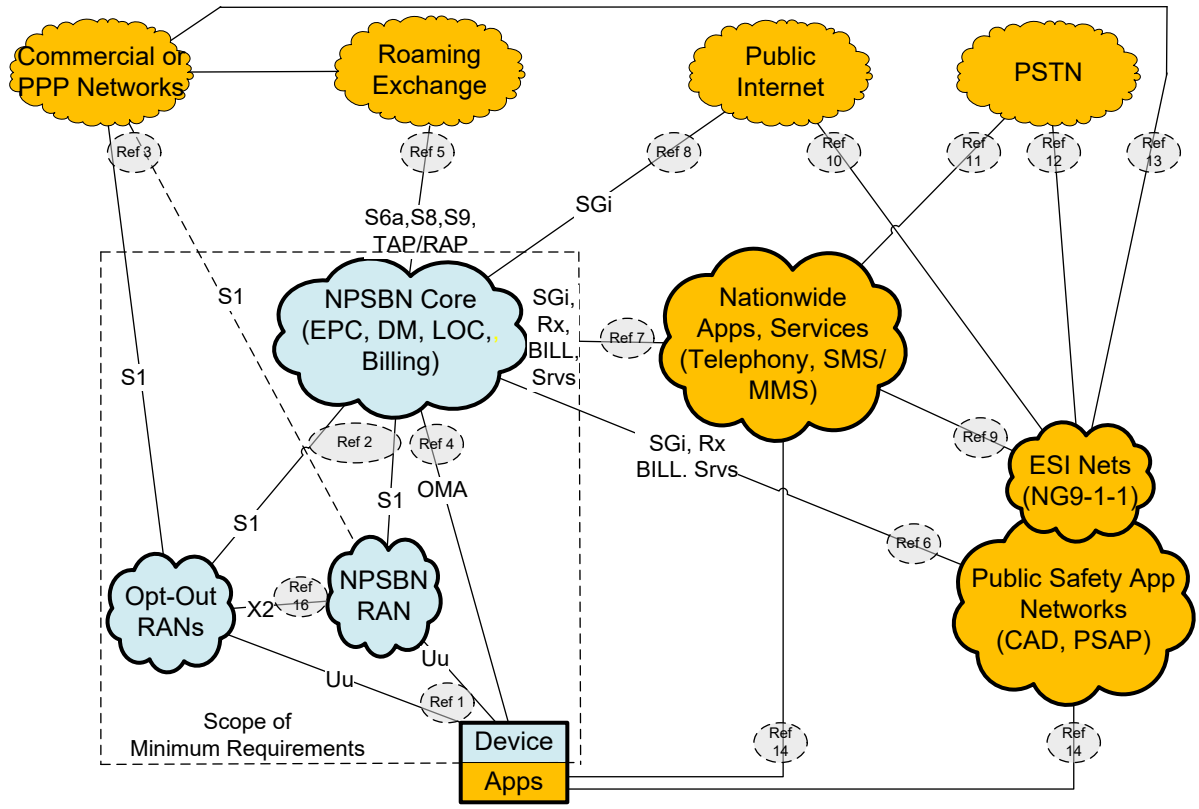


Figure 2: NPSBN Landscape Model

4.1.3 Mapping to 3GPP LTE Reference Architecture

A more detailed view of the LTE interfaces that are contained within the ~~in~~-scope" clouds can be represented by stage-2 level standards reference architecture. A detailed view of the EPC and RAN components are shown in the figure below. This figure was adapted from 3GPP 23.401, Section 4.2.

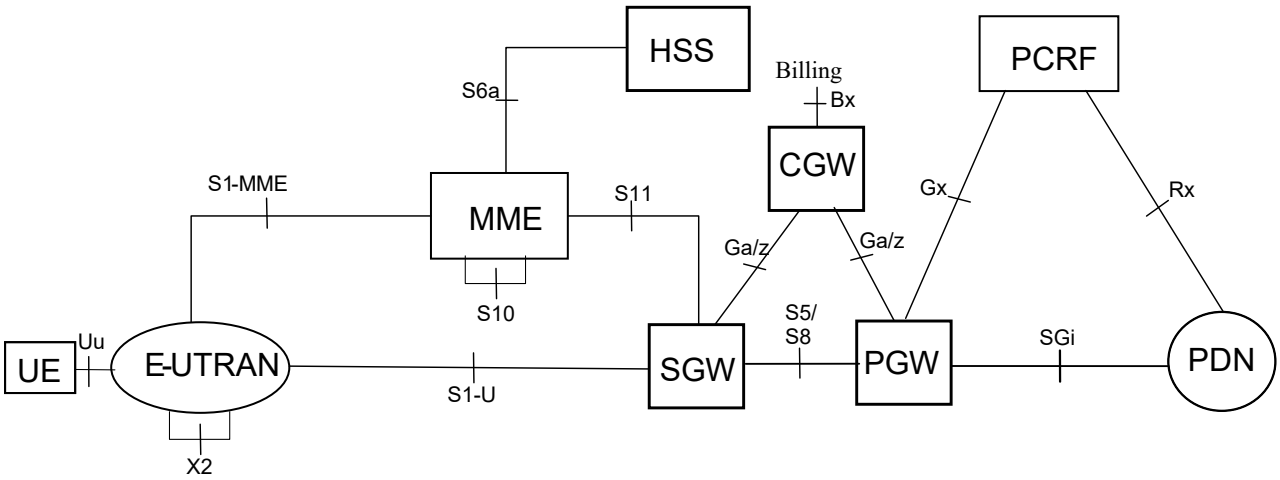


Figure 3: 3GPP LTE Reference Architecture

4.1.4 Existing Infrastructure Integration Scenarios

Spectrum Act section 6206(c)(3) stipulates ―Leveraging Existing Infrastructure … the First Responder Network Authority shall enter into agreements to utilize, to the maximum extent economically desirable, existing – (A) commercial or other communications infrastructure; and (B) Federal, State, tribal, or local infrastructure.‖ The Interoperability Board concluded that this stipulation may require the First Responder Network Authority under section 6206(b) Duty and Responsibility to Deploy and Operate a Nationwide Public Safety Broadband Network, to consider leveraging existing infrastructure. In accordance with this conclusion, reference configurations in which existing infrastructure elements (such as the Waiver systems deployed under FCC Order 10-79) deployed prior to the instantiation of the FirstNet Authority can be leveraged into the NPSBN, while meeting the requirements for interoperability, are described herein.[20]

4.1.4.1 Interim Existing Infrastructure Assumptions

1. Existing RAN infrastructure deployed prior to operation of the NPSBN RAN may be integrated with the NPSBN RAN and Core.
2. Existing EPC infrastructure deployed prior to operation of the NPSBN EPC may be integrated into the NPSBN Core.
3. If existing EPC infrastructure elements are integrated into the NPSBN EPC, the existing and NPSBN EPC elements will use a common PLMN ID.

[20] May 2010 FCC Order 10-79.

The following diagram is identical to that shown in Figure 2 except for the addition of existing Core and RAN elements. These elements and their associated interfaces are included to provide a broader NPSBN landscape context. Existing Core and RAN infrastructure elements are anticipated to be either assimilated into the NPSBN or deprecated over time. For this reason, the existing Core and RAN infrastructure components are identified separately in this interim context.

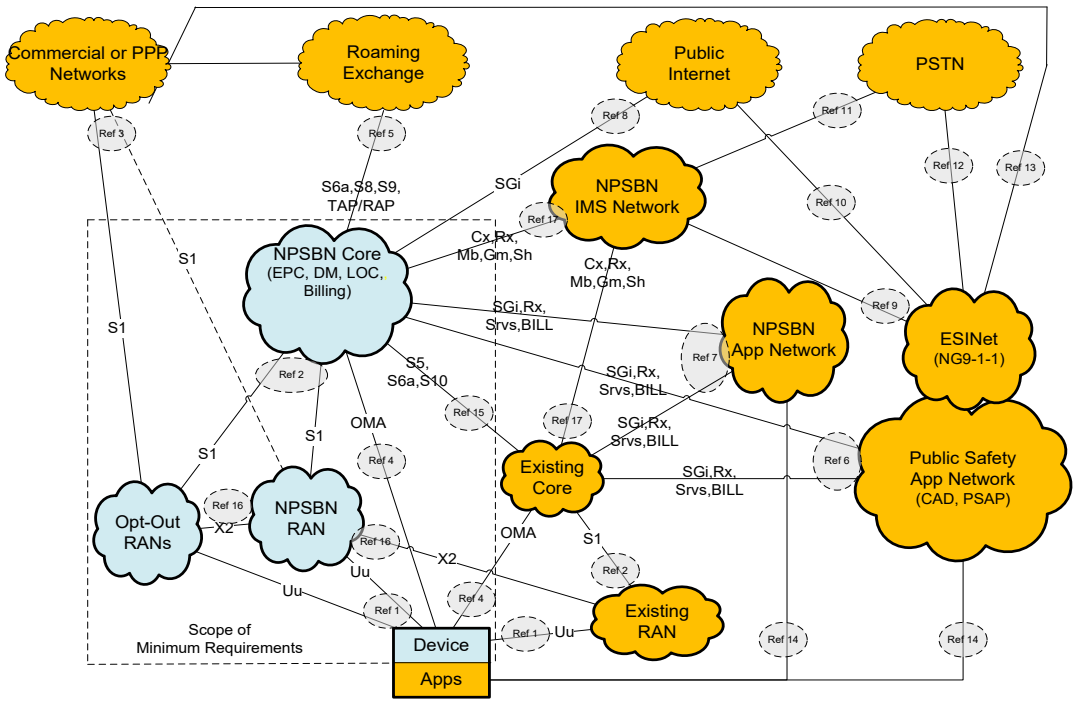
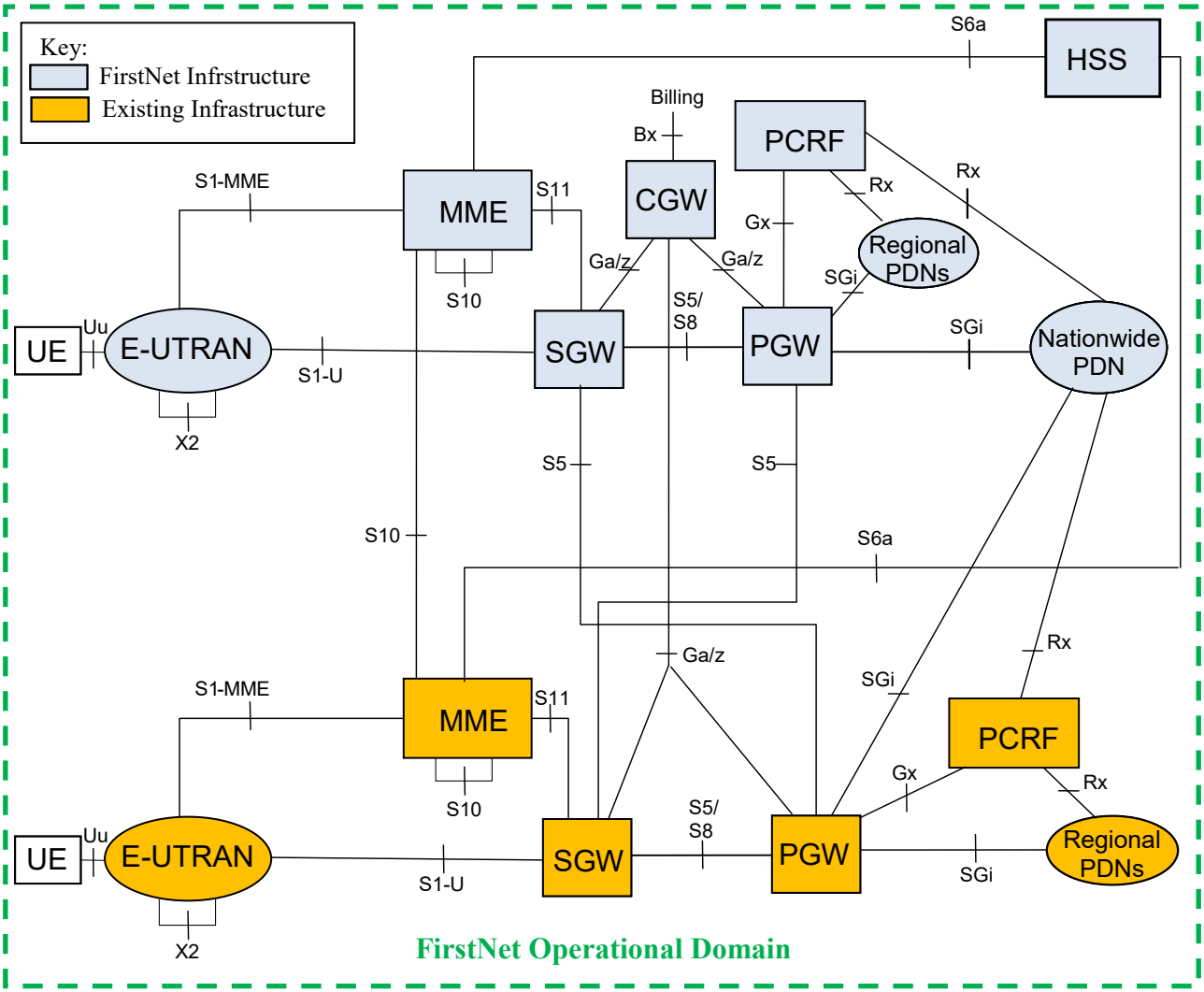


Figure 4: NPSBN – Interim Infrastructure Landscape Model

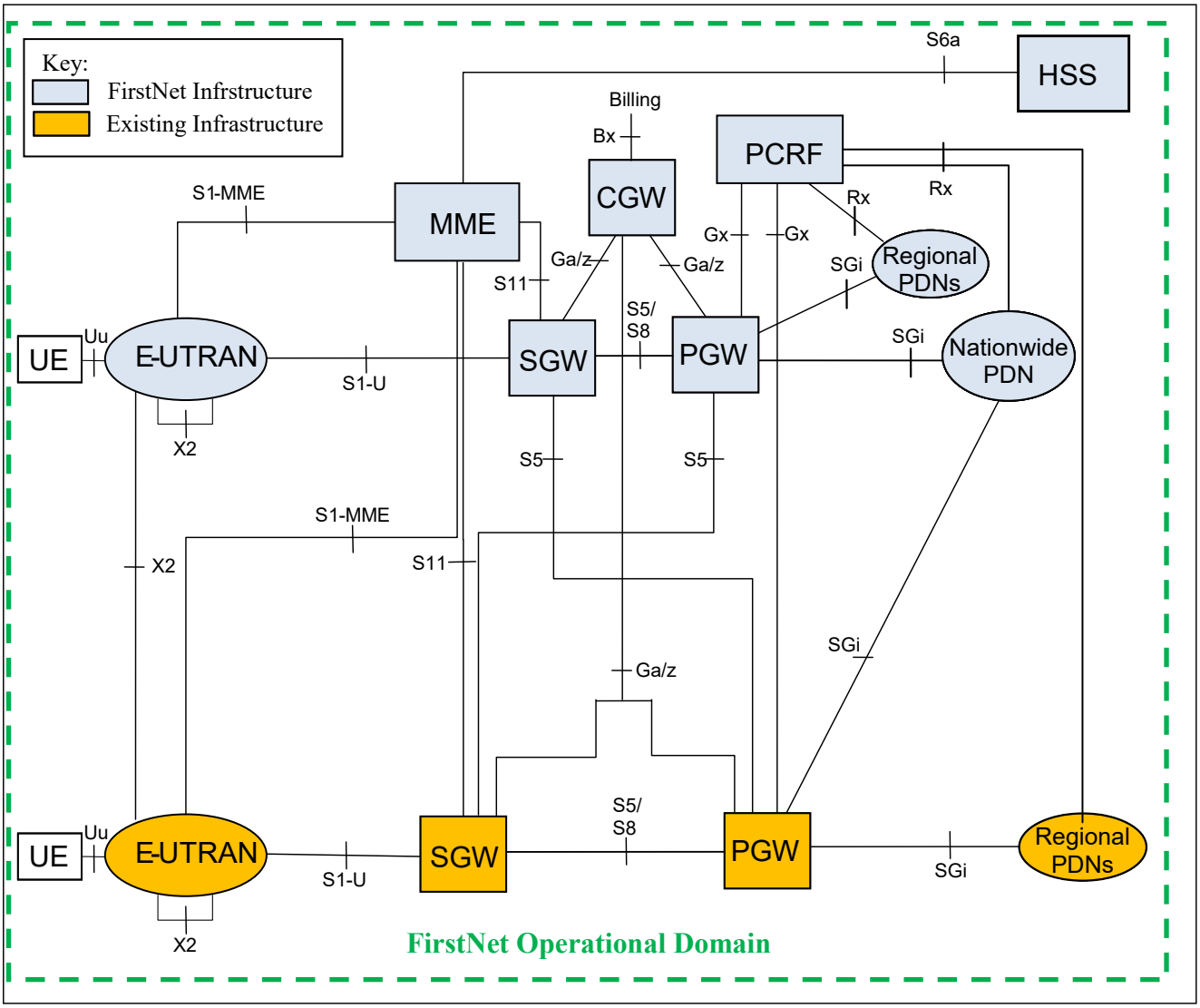
4.1.4.2 Configuration 1 – Leverage User Plane and Signaling Plane Elements of the Existing Infrastructure Networks

In this example, the existing UEs, E-UTRAN (a.k.a, RAN), MME, S-GW, P-GW, PCRF, and Regional Packet Data Networks (PDNs) are integrated into the NPSBN. One logical HSS would exist so the existing HSS's would not be integrated into the NPSBN. The interfaces which extend between the NPSBN elements and the existing infrastructure elements are S5, S6a, S10, SGi, and Rx.



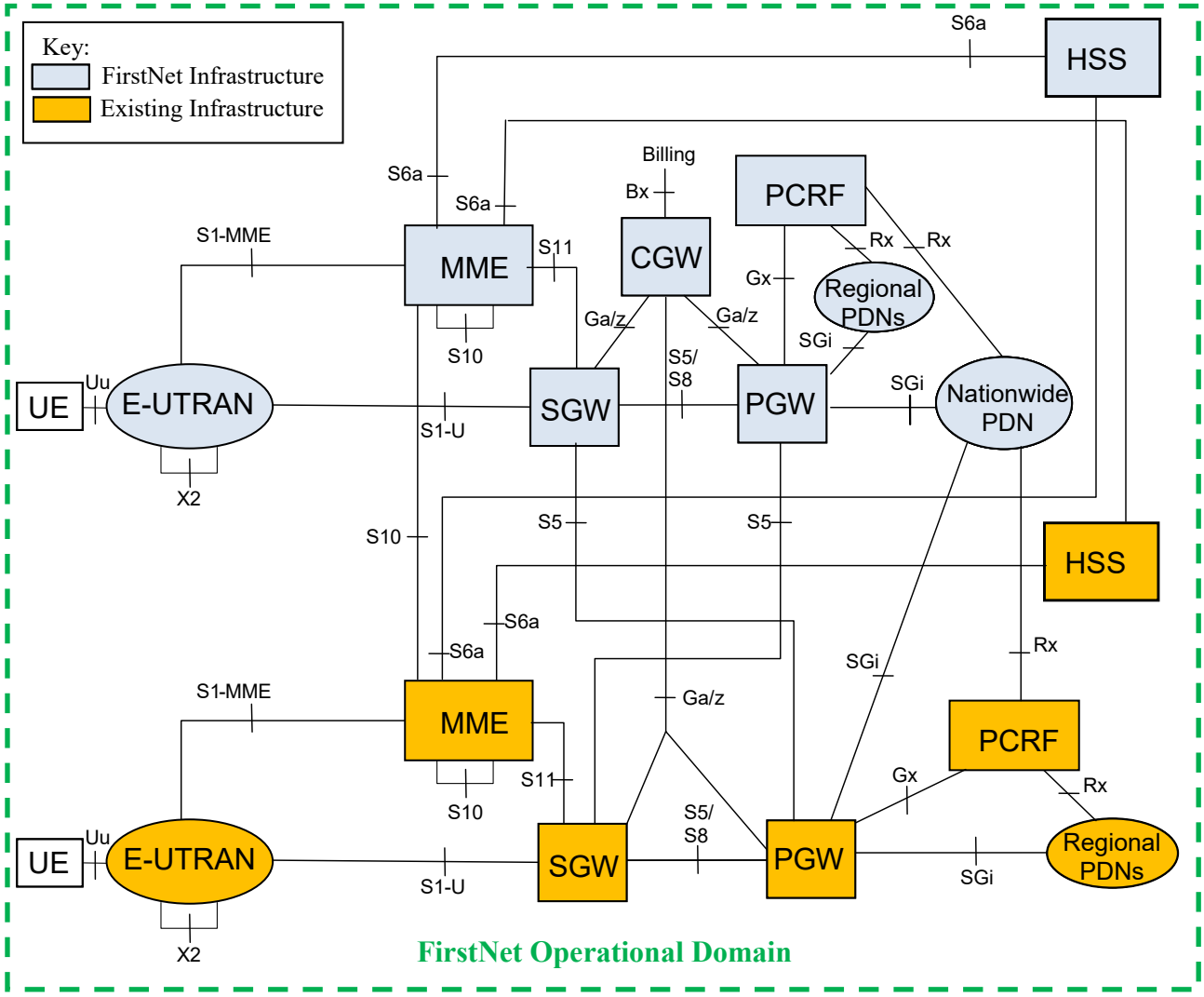
4.1.4.3 Configuration 2 – Leverage User Plane Elements of the Existing Networks

In this example, the existing UEs, E-UTRAN (a.k.a, RAN), S-GW, P-GW, and Regional Packet Data Networks (PDNs) are integrated into the FirstNet-procured NPSBN. Only one logical HSS and one logical PCRF would exist in the NPSBN, however, so these network elements of the existing networks would not be integrated into the NPSBN. The interfaces which extend between the FirstNet elements and the existing infrastructure elements are S1-MME, S5, S11, SGi, and Rx.



4.1.4.4 Configuration 3 – Leverage User Plane, Signaling Plane, and HSS Elements of the Existing Networks

In this example, the existing UEs, E-UTRAN (a.k.a, RAN), MME, S-GW, P-GW, PCRF, HSS, and Regional Packet Data Networks (PDNs) are integrated into the FirstNet NPSBN. Multiple logical HSSs and PCRFs would need to be integrated into the NPSBN. Integrating multiple HSSs into the NPSBN will require support of Diameter Routing Agent functions. Note that these functions would be components of a transport infrastructure and are not illustrated in the diagram. The interfaces which extend between the FirstNet elements and the existing infrastructure elements are S5, S6a, S10, SGi, and Rx.



4.1.4.5 Existing Infrastructure Integration Considerations

Recommended Considerations

(1) Hardware and software systems comprising the NPSBN SHOULD support integration of existing network elements via the necessary commercial standards-defined LTE interfaces enumerated in Table 1: Minimum Interoperable Interfaces.

4.1.5 Interoperable Network Elements

Components depicted in the previous figures are described in the following sections.

4.1.5.1 Device or UE

Spectrum Act section 6206(b)(2)(B) specifies that ―…First Responder Network Authority shall … promote competition in the equipment market, including devices for public safety communications, by requiring that equipment for use on the network be - (i) built to open, non-proprietary, commercially available standards; (ii) capable of being used by any public safety entity and by multiple vendors across all public safety broadband networks operating in the 700 MHz band; and (iii) backward-compatible with existing commercial networks to the extent that such capabilities are necessary and technically and economically reasonable;…" Devices are also referred as User Equipment (UE) in 3GPP parlance.

4.1.5.2 NPSBN RAN

Spectrum Act section 6202(b)(2) indicates that the NPSBN RAN comprises "cell site equipment, antennas, and backhaul…that are required to enable wireless communications with devices…". The RAN utilizes Band 14 radio spectrum.

4.1.5.3 Opt-out RAN

Spectrum Act section 6302(e)(2)(B) allows a state to "conduct its own deployment of a radio access network…".

4.1.5.4 Existing RAN

Identified in the present document as RAN equipment which has been deployed under provisions of the FCC Waiver Orders (e.g. May 2010 FCC Order 10-79). The statute is silent on existing RAN infrastructure; however such assets have been deployed and may be considered for integration into the NPSBN.

4.1.5.5 Public Safety Application Network (PSAN)

PSAN‘s are defined in the present document as State, Regional, Local, Tribal, or Agency application networks which provide public safety services with local scope. Examples of such services are Next Generation Public Safety Answering Points (PSAPs) and Computer Aided Dispatch (CAD). Spectrum Act section 6206(b)(2)(C) directs FirstNet to promote integration of the network with PSAPs.

4.1.5.6 Emergency Services IP Network (ESI Net)

Identified in the NENA i3 architecture as transit networks supporting integration with Public Safety Answering Point (PSAP), ESI Nets are defined in the National Emergency Number Association Interface Standards for Next Generation 9-1-1 (NENA i3). NENA i3 defines an ESI Net as an IP-based inter-network shared by all agencies

which may be involved in any emergency.[21] The i3 Public Safety Answering Point (PSAP) is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the i3 standard.

4.1.5.7 NPSBN Core Network

Spectrum Act section 6202(b)(1) indicates that the NPSBN Core Network comprises the "national and regional data centers, and other equipment … and (B) provides the connectivity between – (i) the radio access network ….

4.1.5.8 Nationwide Public Safety Applications Network (NPSAN)

Spectrum Act section 6202(b)(1) indicates that the NPSBN Core Network (B) provides the connectivity between – (b) the public internet or switched network…". In order to support connectivity to these networks, the FirstNet Applications Network includes Nationwide Applications and Services.

4.1.5.9 Public Internet

Spectrum Act section 6202(b)(1)(B)(ii) indicates that the NPSBN Core Network may provide connectivity to the public Internet.

4.1.5.10 Public Switched Telephone Network

Spectrum Act section 6202(b)(1)(B)(ii) indicates that the NPSBN Core Network may provide connectivity to the public switched network. The Public Switched Telephone Network (PSTN) is an example of a public switched network.

4.1.5.11 Commercial Networks

Spectrum Act section 6206(c)(5) indicates a FirstNet duty to negotiate and enter into roaming agreements with commercial network providers as appropriate. Spectrum Act section 6211 allows the Commission, if necessary, to adopt rules to improve the ability of public safety networks to roam onto commercial networks.

4.1.5.12 Roaming Exchange Networks

Roaming Exchange Networks are identified in the present document as third party service networks required under provisions of the January 2012 FCC Waiver Order DA 12-25. These networks include Internet Packet Exchange (IPX), Data Clearing House (DCH) and Financial Clearing House (FCH) functions, and are commonly used in the commercial industry to support service provider roaming and therefore relevant to the NPSBN Core Network.

4.1.5.13 NPSBN IMS Network

The NPSBN IMS Network is defined herein to support IMS session layer and telephony applications. The NPSBN IMS Network may be considered to support connectivity to the PSTN, although other alternatives are possible. IMS is a 3GPP standardized technology that is being adopted by service providers and, coupled with VoLTE, would be a reasonable foundation for FirstNet to consider should it decide to introduce voice telephony services and applications into the NPSBN.

4.1.6 Reference Point Descriptions

[21]National Emergency Number Association Technical Committee. NENA Functional and Interface Standards for Next Generation 9-1-1. December 2007. Version 1.0 (i3) at http://www.nena.org/?TechnicalStandards.

4.1.6.1 Ref 1 - Reference point between Device and RANs

Ref 1 supports radio connections between Devices and the NPSBN RANs via the 3GPP Uu air interface operating in Band 14. This reference point supports all types of Devices and RANs permissible in the NPSBN.

4.1.6.2 Ref 2 – Reference point between NPSBN Core and RANs

Ref 2 supports the backhaul connections between the NPSBN Core and RANs via the 3GPP S1-U and S1-MME interfaces. The S1-U interface carries User Plane traffic between the eNB and S-GW. The S1-MME interface carries Signaling Plane traffic between eNB and MME.

4.1.6.3 Ref 3 – Reference point between RANs and Commercial/PPP Networks

Ref 3 is similar to Ref 2 in that it supports the backhaul connections and it relies on the same 3GPP interfaces as Ref 2. However Ref 3 supports backhaul for RAN sharing scenarios implied by statute sections 6302(g)(1), which states that —. A State that chooses to build its own radio access network shall not provide commercial service to consumers or offer wholesale leasing capacity of the network within the State except directly through public-private partnerships for construction, maintenance, operation, and improvement of the network within the State." and 6208(a)2(B)(i) which provides for —. access to network capacity on a secondary basis for non-public safety services …"

4.1.6.4 Ref 4 – Reference point between NPSBN Core and Device

Ref 4 supports the Device Management and Device Location services of the NPSBN Core. Device Management functions should minimally include inventory information retrieval, configuration, lock and wipe, and firmware updates. Device configuration should minimally include connection management aspects of LTE (e.g. APNs), application services, and additional access networks (e.g. WLAN). Device Location functions should minimally include secure user plane positioning methods, multiple radio access technologies (e.g. LTE, 3G, WLAN), and roaming support.

4.1.6.5 Ref 5 – Reference point between NPSBN core and IPX, DCH, and FCH service providers

Ref 5 supports roaming with commercial service provider networks and potential Public-Private Partnership (PPP) networks. Typical commercial network practice is to utilize third party service providers to support the roaming functions; however –direct" network-to-network interfaces can be implemented without the use of third party service providers. Roaming functions include User Plane routing, Signaling Plane routing, and Transfer/Return Accounting Procedures. User Plane routing is required for the S8 interface. Signaling Plane routing is required for the S6a and S9 interfaces. The Transfer Accounting Procedure (TAP) and Returned Accounting Procedure (RAP) are required for the GSMA data clearing and financial clearing functions.

4.1.6.6 Ref 6 - Reference point between Public Safety Application Networks (PSANs) and NPSBN Core or Existing Cores

Ref 6 supports public safety applications such as Computer Aided Dispatch (CAD) and Public Safety Answering Point (PSAP) applications using the NPSBN. Reference point 6 is supported by the 3GPP _Rx' interface, the 3GPP SGi interface, the BILL reference point, and a collection of Service (Srvs) oriented interfaces. The SGi carries User Plane application data traffic between the public safety application servers and the NPSBN/existing Core. Within the User Plane of SGi, users authenticate to applications. In order to ensure interoperable access to applications a common framework to identify users is enabled by using standards-based identity protocols such as Security Assertion Markup Language (SAML). The BILL interface carries formatted charging detail records to enable billing functions to be implemented as part of the application networks. The Srvs is defined in the present document as a collection of miscellaneous interfaces to support NPSBN subscription provisioning and Application Programming Interfaces for applications to request QoS policy and charging control from the NPSBN/existing Core. The Srvs interfaces may be specified by Standards Development Organizations other than 3GPP. The Rx

interface enables applications to request QoS policy and charging control from the NPSBN/existing Core.

4.1.6.7 Ref 7 - Reference point between Nationwide Public Safety Application Network (NPSAN) and NPSBN Core or Existing Cores

Ref 7 is similar to Ref 6, except that Ref 7 supports nationwide public safety applications such as Telephony and SMS/MMS applications using the NPSBN. Reference point 7 is supported by the same interfaces as Ref 6.

4.1.6.8 Ref 8 - Reference point between NPSBN Core and Public Internet

Ref 8 supports Public Internet access to/from the NPSBN Core for User Plane connectivity with the NPSBN Devices. This reference point is supported by the 3GPP SGi interface.

4.1.6.9 Ref 9 - Reference point between Nationwide Public Safety Application Network and ESI Net

Ref 9 supports 9-1-1 calls originated by secondary users on the NPSBN to be routed to the ESI Net. The ESI Net completes the call routing to a regional PSAP. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.10 Ref 10 - Reference point between ESI Net and Public Internet

Ref 10 supports incident reports originated from Internet-based applications to be routed to the ESI Net. The ESI Net completes the call routing to a regional PSAP. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.11 Ref 11 - Reference point between NPSBN IMS Network and Public Switched Telephone Network

Ref 11 supports Public Switched Telephone Network (PSTN) access for NPSBN UEs via a nationwide telephony application and an interface between the telephony application and the PSTN. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate potential relationships among networks which are peripheral to the NPSBN.

4.1.6.12 Ref 12 - Reference point between ESI Net and PSTN

Ref 12 supports routing 9-1-1 calls originated from the PSTN to regional PSAPs. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.13 Ref 13 - Reference point between ESI Net and Commercial or PPP networks

Ref 12 supports routing 9-1-1 calls originated from the Commercial or PPP Networks to a regional PSAP via ESI Nets in accordance with the NENA i3 architecture. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.14 Ref 14 – Reference point between Device Applications and Application Managers

Ref 14 supports download, upgrade, configuration, and deprecation of application software residing on Devices via

application managers in the Nationwide Public Safety Application network and in the Public Safety Application Networks. This reference point is not part of the NPSBN. It has been included here to provide a complete landscape and illustrate relationships among networks which are peripheral to the NPSBN.

4.1.6.15 Ref 15 - Reference point between NPSBN Core and Existing Core

Ref 15 supports Device access, mobility, and handover between the NPSBN Core and existing Cores.

4.1.6.16 Ref 16 - Reference point between E-UTRANs

Ref 16 supports inter-eNB handovers. As such, X2 is beneficial only between eNBs that provide adjacent RF coverage. As of 3GPP release 10, the X2 handover procedures are limited to cases where the MME is unchanged during the handover; that is, handover between eNBs which are connected to a common MME. The S1-based handover procedure is used when the X2-based handover cannot be used.

4.1.6.17 Ref 17 - Reference point between NPSBN IMS Network and NPSBN Core or Existing Cores

Ref 17 supports IMS session and telephony services for the NPSBN Core and Existing Cores. Ref point 17 is supported by the Cx, Gm, Mb, Rx, and Sh, interfaces. The Cx interface provides support for storage/retrieval of IMS-related subscription and routing information stored in the HSS. The Gm interface provides support for SIP-related signaling with the UE. The Mb interface provides support for bearer traffic between the UE and IMS applications. The Rx interface enables IMS applications to request QoS policy and charging control from the NPSBN or Existing Core. The Sh interface provides for storage/retrieval of IMS application-specific information stored in the HSS.

4.1.7 Minimum Required Interoperable Interfaces and Standards

The table below enumerates minimum interoperable interfaces and standards associated with the NPSBN. Note that the standards referenced herein are relevant at the time of this writing. These standards are required to be supported as long as they are relevant to the NPSBN. However, it is recognized that standards evolve over time and hence it is expected that the standards enumerated in this table may be deprecated and/or replaced in the future.

Table 1: Minimum Interoperable Interfaces

Interface Name	Description	Required Standards
Uu	Air Interface between Device (aka, UE) and eNB.	3GPP TS 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.314, 36.321, 36.322, 36.323, 36.331
S1	Comprised of two interfaces: S1-U user plane between eNB and S-GW; S1-MME signaling plane between eNB and MME, UE and MME.	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.412, 36.413, 36.414, 33.210, 33.310
S6a	Signaling plane interface between MME and HSS.	3GPP TS 29.272
S5/S8	User plane interface between S-GW and P-GW.	3GPP TS 29.274, 29.281
S9	Signaling plane interface between PCRF in home network and PCRF in visited network.	3GPP TS 29.215
S10	Signaling plane interface between MMEs.	3GPP TS 29.274
S11	Signaling plane interface between MME and S-GW.	3GPP TS 29.274
SGi	User plane interface between P-GW and external IP networks.	3GPP TS 29.061
Gx	Signaling plane interface between PCRF and P-GW.	3GPP TS 29.212, 29.213
Rx	Signaling plane interface between PCRF and external Application Functions.	3GPP TS 29.214
X2	User plane and Signaling plane interface between eNBs.	3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424

4.1.8 Recommended Requirements for Interface Interoperability

LTE interfaces evolve over time. Therefore in developing recommendations based on these evolving interfaces, it is important to give precedence to standardized LTE interfaces that are deployed in commercial practice over those that are earlier in the evolution process. Furthermore, as FirstNet designs and deploys the NPSBN, the Interoperability Board recognizes the possibility that required functions and interfaces that don‘t exist within available LTE standards will arise. To that end, in developing its recommendations, the Interoperability Board includes the following methodology that prescribes precedence ordering for selection of standards and interface specifications for use in the NPSBN. The intent of this precedence ordering is that succeeding steps are only executed when reasonable options do not exist with preceding steps.

Table 2: Standards Implementation Methodology

Step 1.	Implementation based on open, consensus-based, non-proprietary, commercially available standards, commonly used by commercial service providers
Step 2.	Implementation based on open, consensus-based, non-proprietary, commercially available standards established for use by commercial service providers
Step 3.	Implementation based on the development and adoption of open, consensus-based, non-proprietary, commercially available standards within recognized standards setting organizations, through direct participation in these standards-setting activities by FirstNet
Step 4.	FirstNet may implement a solution based on open specifications available to all authorized parties

[1] Hardware and software systems comprising the NPSBN SHALL implement interfaces consistent with Table 2: Standards Implementation Methodology.
[2] Hardware and software systems comprising the NPSBN SHALL support the interfaces enumerated in Table 1: Minimum Interoperable Interfaces.
[3] Hardware and software systems comprising the NPSBN SHALL support management functions.
[4] Hardware and software systems comprising the NPSBN SHALL support APNs defined for PSAN usage.
[5] Hardware and software systems comprising the NPSBN SHALL support nationwide APNs for interoperability.
[6] Hardware and software systems comprising the NPSBN SHALL enable QoS control for PSAN-hosted applications via the 3GPP _Rx' interface.
[7] The NPSBN SHALL support IPv4, IPv6, and IPv4/v6 PDN types defined in 3GPP TS 23.401.
[8] The NPSBN SHALL support IPv4 and/or IPv6 transport for the EPS interfaces enumerated in Table 1: Minimum Interoperable Interfaces, consistent with the FirstNet design.
[9] Any sharing agreement that FirstNet enters into SHALL implement network sharing according to 3GPP TS 23.251 and SHALL NOT impact public safety operations.

4.1.9 NPSBN Services Offered to Applications

The NPSBN would benefit from implementing a set of common nationwide network services which can be accessed by applications and used in a standard and interoperable manner. Examples of such services are Billing, Short Message Service (SMS) messaging, Location, Presence, and Device Management. These services are typically not directly visible to end-users, but rather made available to end-user applications or administrative-user applications.

In the commercial service provider environment, these services are typically based on standards; however, each network service provider tends to select unique standard options that best fits its needs. As a result, there are multiple standards-based options to realize such services. For this reason, there are multiple _state-of-the-art' practices that could be leveraged by the NPSBN. This situation will require FirstNet to select specific standards-based options to implement these services. After specific options are selected, these services can be deployed while maintaining interoperability within the NPSBN context. While not universal among service providers at this writing, IMS offers a useful standards framework for FirstNet to consider for implementation of these services.

4.1.9.1 Billing Capability

The ability to receive billing information from the NPSBN will be essential to the success of the network. Public Safety has unique charging scenarios (jurisdictional charging, investment credits, mutual aid, regional users, etc.), and each local entity and/or regional entity typically sets its own policies for these charging scenarios. Consolidated public safety systems (referred to in this section as regional entities) will need the ability to efficiently and accurately identify charges to the appropriate ―cost causer" and receive the appropriate data that will enable the ―re-billing" of charges. It is important that FirstNet agree to publish billing records directly to local entities (format TBD, but potentially TAP3 or CDRs) for all charges that will be passed on to these local/regional entities. It is important that this function be performed in the most economical way possible, without additional ―per transaction" costs.

Billing becomes a technical requirement because of the way most consolidated/regional systems are funded. For example, in the majority of state governments across the country, the IT organizations are established under a charge-back-for-services model. The agencies receive little or no funding from their respective Legislature, and sustainability of the services offered is accomplished through a fee for service. IT organizations purchase or create services at discounted pricing and ―re-sell" these services to their customer base at a price that covers their cost of providing the service. Rates for services must comply not only with individual state laws, but with Federal OMB Circular A-87 rules and regulations. These regulations assure that neither the state nor the federal government customers pay more than their ―fair share" of the charges. Therefore it is extremely important that these types of organizations can identify the appropriate entity/person to re-bill. Currently, all state government IT organizations are billing clients for network services that include data (broadband), voice and video. Additionally, several of these same entities currently re-bill services for their state land mobile radio services.

The unique charging scenarios for public safety are mostly ignored by service-provider-focused billing vendors. In fact, the current emphasis by commercial service-provider-focused billing vendors on real-time billing, used today primarily to enforce usage limits, is mostly unhelpful to public safety.

The ability of local/regional entities to work with FirstNet to ensure billing is provided to meet their unique environment will ensure that they can produce one integrated invoice per-user or per-agency for their public safety LTE and other local Entity services.

Recommended Considerations

(2) Billing information from the NPSBN SHOULD be provided to each local and/or regional entity for the NPSBN services.

4.1.9.2 Location Based Data Capability

Location data should be accessible to appropriate applications and only the appropriate end users, as may be authorized by management level policy. Location data applications may be on both UE's and associated agency level command/control applications. UEs of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is applicable on commercial services networks in order to retain a broad level of compatibility with incumbent systems.

The LTE standards support several methods of locating devices using GPS or network assisted calculation methods. Use of a network assisted location service does not need to be limited to just working over LTE and can additionally report location using 3G or Wi-Fi access. If additional location coverage is desired beyond GPS, network assisted location will need to be part of an evolution plan for the network services layer.

There are several methods to implement the signaling of location information between the UE and the network. The two methods generally implemented are control plane solutions based on 3GPP TS 23.271 or a user plane solution based on OMA (Open Mobile Alliance) Secure User Plane Location (SUPL). The user plane solution is referenced from 23.271 but the details are covered in OMA specifications. A service provider typically chooses a single

method to deploy in their network.

Recommended Requirements

[10] The NPSBN SHALL include the capability to collect and convey UE location data to applications using a standardized interface in near real time.

4.1.10 Network Applications

4.1.10.1 Recommended Minimum Requirements

A number of the applications specified by the National Public Safety Telecommunications Council (NPSTC) Broadband Task Force indicated below can be supported with best-effort IP data access – a service that will be available on all initial and subsequent LTE network deployments. In the commercial world, such applications are known as ―Over the Top Applications", referring to their ability to run on top of a best-effort IP data service without requiring additional integration effort at the network transport layers. Data applications currently used by public safety agencies that run over commercial service provider networks, for example, operate as ―Over the Top Applications." These applications can be readily migrated to the public safety wireless broadband network, leveraging existing applications, procedures, processes and expertise. All Over the Top Applications can be further enhanced through the use of priority services, services that require the exchange of signaling messages between the LTE network and application to allow the application to request a specific priority treatment. The use of Over the Top applications will have an impact on network capacity requirements and perhaps other aspects of the LTE network as it evolves. LTE is further anticipated to greatly increase mobile video usage within the public safety workflow. Enhanced support for this and other applications through the introduction of QoS, priority services or other supplemental security services that are required by public safety must be considered as part of the network evolution plan.

Recommended Considerations

(3) The NPSBN SHOULD support existing Public Safety applications, deployed regionally or within agencies.

4.1.10.1.1 Internet Access

The NPSTC Broadband Task Force report recommends that support of internet access be required on all LTE networks deployed. This access can come directly or via access to a home network with internet connectivity. Many of the home network services are only available on the agency private network and would better be served with private connectivity to the agency. Private connectivity allows for priority/QoS to be applied. Connectivity through the internet normally implies best effort only.

Recommended Requirements

[11] The NPSBN SHALL be capable of providing public safety subscribers with access to the global Internet.

4.1.10.1.2 Information "Home page"

The NPSBN may be required to provide public safety a universal method to obtain a "home page" for visitors to the system. This "home page" will facilitate access to and distribution of available applications, alerts, incident specific information, system status information, and information that the service provider deems important to share with visitors to the system.

Recommended Considerations

(4) The NPSBN SHOULD provide a method to connect a device to a packet data network where a ~~h~~home page" application is hosted with location specific content.
(5) The NPSBN SHOULD provide a method where a ~~h~~home page" application is available via an alternate access network, other than the NPSBN. This is a recommendation that the home page be made available and location-aware while roaming or over Wi-Fi.
(6) The NPSBN SHOULD provide a specification for locating a ~~h~~home page" based on current or manual location.

4.1.10.1.3 Field-Based Server Applications

Recommended Considerations

Public safety users have the need for client devices to consistently and continuously reach server-based applications that may be hosted in jurisdictional networks or accessible via the global internet. Field-based server applications include, for example, Computer-aided Dispatch (CAD) and Records Management Systems (RMS).

(7) The NPSBN SHOULD support use of field-deployed server applications.
(8) The NPSBN SHOULD support devices that are reachable via the global internet and can be used to host field based server applications (i.e. deployable servers).

4.1.10.1.4 Access to Responders under Incident Command System (ICS)

Recommended Considerations

(9) The NPSBN SHOULD allow the devices outside of their normal jurisdiction to connect to a local packet data network and to the device's home packet data network to carry out incident objectives.

4.1.10.1.5 Status/Information "SMS-MMS Messaging"

Recommended Considerations

(10) The NPSBN SHOULD provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages.

4.1.10.1.6 PSTN Voice

PSTN Voice refers to the ability of the NPSBN to support telephony services; both mobile-to-mobile and mobile-to-land. Because LTE is a packet-only technology, some form of additional voice-over-IP technology is necessary to support telephony services. While not required by the Spectrum Act, it is envisioned that the NPSBN will support telephony services at some point in the future. Commercial service provider support for telephony services over LTE is anticipated in the near future. However, as of this writing, commercial service providers in the U.S. have not commercially deployed an LTE telephony solution, and thus it is not prudent to require FirstNet to advance ahead of commercial service provider deployments with this technology.

In addition, there may be several public safety specific issues which need to be resolved in order to provide PSTN voice service via the NPSBN. Examples of these issues are:

- Precedence of a 911 call vs. a first responder PTT emergency call
- End-to-end signaling confidentiality to avoid exposing responder-specific information
- Session continuity when roaming to avoid dropped calls

- Pre-emption of secondary users during congestion (including 911 and CALEA calls)
- Selective logging of calls for evidentiary purposes
- NAT traversal across various network segments (including Opt-Out) in the NPSBN

One application that warrants special attention when roaming is Voice over LTE (VoLTE). VoLTE can be used in the NPSBN to provide cellular type telephony services similar to voice services provided today in commercial mobile networks. Support of telephony voice services on the NPSBN has been called out in a number of practioner-driven requirements efforts, including NPSTC's Broadband Statement of Requirements.[22] Note VoLTE is distinct from the PTT/MCV application additionally required by public safety. VoLTE is an IMS application as defined by 3GPP TS 22.173 and follows the "IMS profile for voice and SMS" as defined in GSMA IR.92. When roaming from the NPSBN to commercial LTE networks, a roaming user should be able to establish calls as long as the roaming LTE network provides support for VoLTE. Note, if a user leaves the NPSBN while on a VoLTE call, the call will drop, requiring the user to re-establish the call on the roaming network. The initial application of VoLTE on the NPSBN will therefore be less functional than the application of VoLTE in a commercial network where a service provider can leverage techniques such as Single Radio Voice Call Continuity (SRVCC) to hand over to other radio technologies. Consequently deployment of VoLTE may need to wait for a region to have significant NPSBN coverage. Also, the new network may not have the bandwidth available to continue previous services such as video sessions with the same QoS. Additionally the NPSBN may need to support E911 calling for secondary users of the NPSBN, including support for location, and possibly CALEA.

If roaming to non-LTE commercial networks the user device will require the support of the appropriate voice solution used in the specific network it is roaming onto in order to make cellular type telephony calls.

Recommended Considerations

(11) Voice Sessions SHOULD be handed off within the NPSBN with limited delay and loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature is a future evolution capability.

(12) The NPSBN SHOULD support Voice over LTE (cellular voice) capabilities using GSMA PRD IR.92.

4.1.11 Additional Recommended Reference Points and Standards

The table below enumerates additional interoperable reference points and standards which are recommended to be implemented within the NPSBN. These reference points are not part of the recommended minimal technical requirements because they are either emerging at the time of this writing or have not been widely adopted in the industry. When available, these interfaces should be implemented with open, consensus-based, non-proprietary, and commercially available standards.

Table 3: Reference Points and Standards

Ref Name	Description	Recommended Standards
OMA	Collection of Device related service interfaces supporting Location (LOC) services, and Device Management (DM) services.	Device Management services should comply with the following OMA-DM requirements and Enabler Test Specifications (ETS): • Basic protocol v1.2, Acc, DevInfo, DevDetail as specified in OMA-RD-DM-V1_2-20070209-A (requirements) OMA-ETS-DM-V1_2-20110128-C (enabler test spec). • Firmware Update Management Object (FUMO) as specified in

[22] NPSTC, Public Safety 700MHz Broadband Statement of Requirements – Version 0.6, November 8th, 2007.

		OMA-RD-DM-V1_2-20070209-A (requirements) OMA-ETS-FUMO-V1_0-20101125-C (enabler test spec). • Lock and Wipe Management Object (LAWMO) as specified in OMA-RD-LAWMO-V1_0-20080610-C (requirements) It should be noted that LAWMO is an emerging specification and does not yet have an associated Enabler Test specification which has been approved for release. However, this should be adopted if/when such specification becomes available in the future. • Connection Management Object (ConnMO) as specified in OMA-RD-ConnMO-V1_0-20081024-A (requirements). It should be noted that although ConnMO has been approved for release, it is comprised of a large number of optional sub-components and it does not have an associated Enabler Test specification defined. FirstNet should develop certification spec that details the required ConnMO object instances. Location Services should comply with the following 3GPP and OMA location specifications: • 3GPP TS 36.355 (LTE positioning protocol) • Secure User Plane Location protocol as specified in OMA-RD-SUPL-V3_0 (requirements) OMA-AD-SUPL-V3 (architecture) OMA-ERELD-SUPL-V3_0 (enablers) OMA-TS-ULP-V3_0 (user plane protocol) • Mobile Location Protocol services as specified in OMA-RD-MLS-V1_3 (requirements) OMA-AD-MLS-V1_3 (architecture) OMA-ERELD-MLP-V3_1 (enablers) OMA-LIF-MLP-V3_3 (mobile location protocol) OMA-TS-LPPe-V1_1 (LPP extensions)
Srvs	Server Side QoS Interfaces for LTE Aware Applications	Applications that require/desire specific bearer QoS or priority should use the Rx interface. API services for Web-based applications should comply with the emerging open, consensus-based, non-proprietary, commercially available standards.
	Server Side QoS Interfaces for Over the Top Applications	These applications are outside the scope of this document, and can continue to use the interfaces used today.
	Subscriber Provisioning services	Subscriber Provisioning enables subscriptions to be added, modified, or deleted from subscription databases within the NPSBN/existing Cores. Subscriber Provisioning includes provisioning portals which enable agencies to manage subscriptions for their users. These capabilities are not supported by commercial standards. Therefore, NPSBN-specific interfaces will be required to support this functionality.
	Identity Management and Identity Federation	Public Safety applications should utilize a standardized framework for user identity management based on the Security Assertion Markup Language (SAML). SAML identity federation profiles enable users to strongly authenticate to applications and then based on application policies users can be authorized to appropriate levels of access within the application. The SAML v2.0 is recommended and associated specifications are located at http://docs.oasis-open.org/security/saml/v2.0.

		The core SAML specification is Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, 15 March 2005, located at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
TAP/ RAP	Transferred Accounting Procedure / Returned Accounting Procedure	GSMA BA.12 – Transferred Account Procedure and Billing Information GSMA BA.13 - Returned Account Procedure GSMA TD.57 - Transferred Account Procedure Data Record Format Specification Version Number 3
BILL	Accounting and Charging Data Records	The accounting and charging data record interface is specified in 3GPP TS 32.297 and 32.298.
IMS	Collection of interfaces supporting the IMS Session and Telephony services.	The IMS interfaces Cx, Gm, Mb, and Sh are specified in 3GPP TS 23.228

4.2 User Equipment and Device Management

Interoperability in the areas of user equipment and device management is important to the success of the NPSBN. The ability to use devices across the different types of broadband networks (e.g. NPSBN and Commercial Roaming Partner networks) is critical for ubiquitous first responder broadband capabilities. The ability to procure mobile broadband devices from a variety of sources will yield significant cost, functional, and performance benefits. The ability to remotely manage devices over-the-air will simplify operations related to devices.

4.2.1 User Equipment

4.2.1.1 Standards

3GPP provides extensive standards relevant for LTE devices and necessary for interoperability over reference point 1 (see Section 4.1.6.1).

Recommended Requirements

[12] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP Release 9 Uu interface enumerated in Table 1: Minimum Interoperable Interfaces.

[13] All User Devices (UEs) deployed on the NPSBN SHALL conform to the 3GPP TS 36.306 UE Radio Access Capabilities, Release 9.

4.2.1.2 USIM/UICC

In the network architecture of 3GPP, user equipment devices, or user equipment (UE), consist of at least two physically separate elements. The first element is a physically secure element—an Integrated Circuit card, or smart card, called the Universal Integrated Circuit Card (UICC)—that hosts authentication applications, such as the Universal Subscriber Identity Module (USIM), used for accessing services provided by the mobile network. The second element is Mobile Equipment (ME), which includes the radio interface and other mobile network access functions.

FirstNet should leverage existing UICC IOT standards as described by 3GPP PCS Type Certification Review Board (PTCRB) and add specific test cases to enable any specific baseline standardization for the USIM/USAT applications that run on any UICC that will be installed in a public safety device. This will enable public safety entities to source their own UICC (SIM cards) independently and thus will avoid the creation of single source (monopoly) and any perceived bottlenecks for UICC availability. Such a process will also allow the market forces to drive the cost of UICC while making sure that UICC elements have been completely tested to work in commercial service provider networks and the NPSBN.

Recommended Requirements

[14] All User Devices (UEs) SHALL support interworking of the device with the USIM/USAT applications on the UICC in accordance with the relevant 3GPP 31.101, 31.102, and 31.111 standards.

4.2.1.3 Roaming

FirstNet subscribers should be able to obtain service on commercial LTE and 2G/3G networks. FirstNet should establish interoperability requirements related to band class support and network selection for selected classes of UEs. For example, FirstNet might specify handheld User Devices should support Public Safety LTE, one or more Commercial LTE band, and either 3GPP or 3GPP2 bands. These requirements should be verified during Device Certification as defined in Section 4.3.2.

FirstNet should ensure that its devices enable FirstNet to enter roaming agreements and public-private partnership

arrangements with any commercial service provider and allow FirstNet users to obtain service in those commercial networks. A device that is capable of obtaining such service in certain bands shall operate on all FirstNet roaming partner networks operating in those bands and not be locked to a subset of FirstNet roaming partner networks operating in those bands.

Recommended Requirements

[15] All User Devices (UEs) deployed on the NPSBN that support roaming onto commercial LTE networks SHALL operate on any FirstNet roaming partner network using bands supported by the device.

4.2.1.4 Public Safety Specific Device Performance

Section 4.6 outlines the Grade of Service required for public safety, including coverage areas for the NPSBN. In order to meet the necessary grade of service, public safety entities may require devices with higher than typical transmit power (e.g. vehicular modems) to expand coverage and minimize the required number of eNBs. This can also have an impact on Grade of Service for low power UEs.

The need to support a mixture of high and low power mobile broadband devices creates unique coverage, capacity, and interference scenarios for the NPSBN. These issues are unique to public safety broadband and not typically experienced in a commercial service provider LTE deployment, thus requiring special consideration by the FirstNet.

Recommended Considerations

(13) The NPSBN SHOULD allow the integration of high power LTE UEs as they become available, based on the methodology contained in Table 2: Standards Implementation Methodology.

4.2.1.5 Future Readiness

It is widely accepted that migration to IPv6 is inevitable for the NPSBN.

Recommended Requirements

[16] All UEs SHALL support dual IPv4/IPv6 stacks.

4.2.2 Device Management

4.2.2.1 Overview

The ability to remotely manage devices over-the-air will simplify operations related to devices. Commercial LTE service providers use a variety of commercially available, standards-based solutions for device management. FirstNet should follow this service provider model.

It has not been determined how device platform management and device application management responsibilities will be divided between FirstNet and the public safety entities. The possible divisions of responsibility include:

- All DM capability is performed by FirstNet, including device platform management and device application management.
- All DM capability is performed by the public safety entities, including device platform management and device application management.
- DM capabilities are divided between FirstNet and the public safety entity. For example, the NPSBN might be responsible for managing a device platform and set of national applications, while the public safety entity is responsible for managing a set of local applications.

The division of responsibility between the public safety entity and FirstNet as well as the specificity of standards prescribed is still to be determined. The DM solution should provide the necessary interoperability to support the three device management models outlined above.

4.2.2.2 Standards

Recommended Considerations

(14) User Devices and Device Management solutions SHOULD support remote management capabilities over-the-air, including software update, discovery, device platform configuration, lock, unlock, wipe, and security configuration.

4.2.2.3 Application Management

As stated in the overview, no determination has been made regarding the divisions of responsibilities between the FirstNet and the local entities for managing applications in devices served by the NPSBN. In order to ensure an interoperable application management capability between the NPSBN and the local entities, FirstNet should define and verify the mechanisms that enable application management by the local entity. Issues that require definition include security requirements, transport requirements, and the method for binding applications to local APNs.

Recommended Considerations

(15) The software systems that comprise the NPSBN SHOULD support the ability to enable local entities to install, update and manage their own applications. This may include security, transport and local APN provisioning.

4.2.3 Subscriber Provisioning

Subscriber management is a critical function of any service provider and is especially important in the NPSBN, where rapid and reliable provisioning of the network and first responder devices is a fundamental capability. While subscriber management is generally considered an operations issue, the subscriber provisioning task must function across the NPSBN and local entity domains and hence impacts interoperability.

It has not been determined how subscriber provisioning will be performed in the NPSBN. FirstNet must provide a mechanism for local entities to independently add and manage subscribers. Independent subscriber management by local entities requires a point of interoperability between the NPSBN and the local entities. It is imperative that the NPSBN includes an interoperable subscriber provisioning function in order to guarantee timely and reliable addition, modification and deletion of subscribers to the NPSBN by the local entities.

To facilitate external provisioning capabilities, a subscriber provisioning interface should be published and version controlled by FirstNet. This enables end to end provisioning regardless of the divisions of responsibilities between FirstNet and the local entity when provisioning subscribers. These interfaces must be verified during interoperability testing.

Recommended Considerations

(16) The software systems that comprise the NPSBN SHOULD provide published and version-controlled subscriber provisioning interfaces to enable end-to-end subscriber provisioning by the local entities. These interfaces SHOULD be verified during interoperability testing.

4.3 Testing

4.3.1 Testing Overview

FirstNet will be deploying a new technology (LTE) with multiple vendors supplying equipment into the ~~"n~~network". Within the network, it is necessary that many elements connect with one another, and each one of these connections must meet a minimum set of specifications to ensure it can interwork with all others. Within the high level 3GPP diagram illustrated in Figure 3 there may be multiple vendors supplying the user equipment (UE), the operating system (OS) on the UE, applications that run on the OS on the UE, eNB antenna electrical down-tilt controllers, EPCs, etc., all the way to the application servers and everything in between. The ability to provide quantitative data for FirstNet for each of these interconnections among network interfaces should be determined by a specific and thorough test regimen that ensures not only interoperability but also operability of the network.

This of course doesn't assume that every piece of equipment deployed in the network itself has been tested. Instead, it is expected that a representative model of equipment has been tested and passed in a controlled environment under predetermined test conditions, before other models of the same type can be deployed in the network.

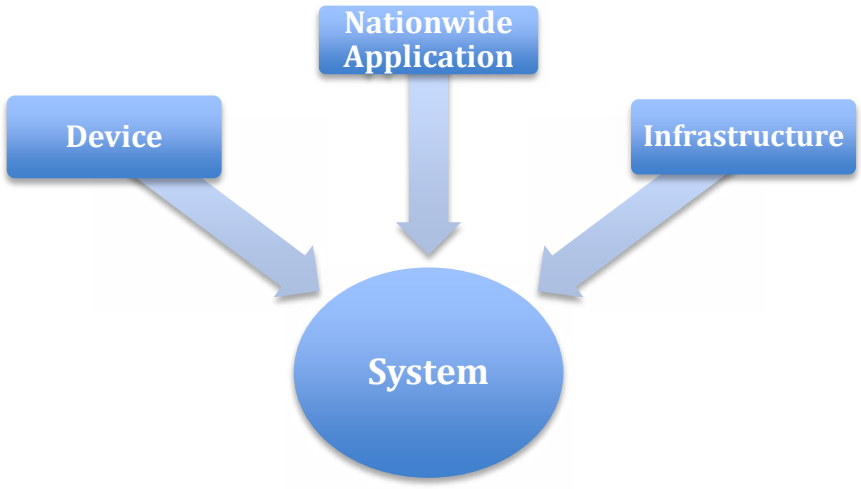


Figure 5: Testing Regimen

Testing can be partitioned into different categories. The entire LTE network or system level tests comprise three main sub-categories of testing: 1) Infrastructure; 2) Devices; and 3) Nationwide Applications. To be able to perform end-to-end system-level tests, each one of the primary subsystems within the network needs to be tested at multiple stages. In order to maximize cost savings, the NPSBN should leverage testing conducted by vendors and existing commercial certification processes.

It should also be recognized that testing is an ongoing activity and not a ~~"o~~nce and done" event. Software updates, bug fixes, new feature releases and introductions, standards updates, new vendors, and many other factors require continual testing to ensure network operability and interoperability. Figure 6 below depicts this testing lifecycle.

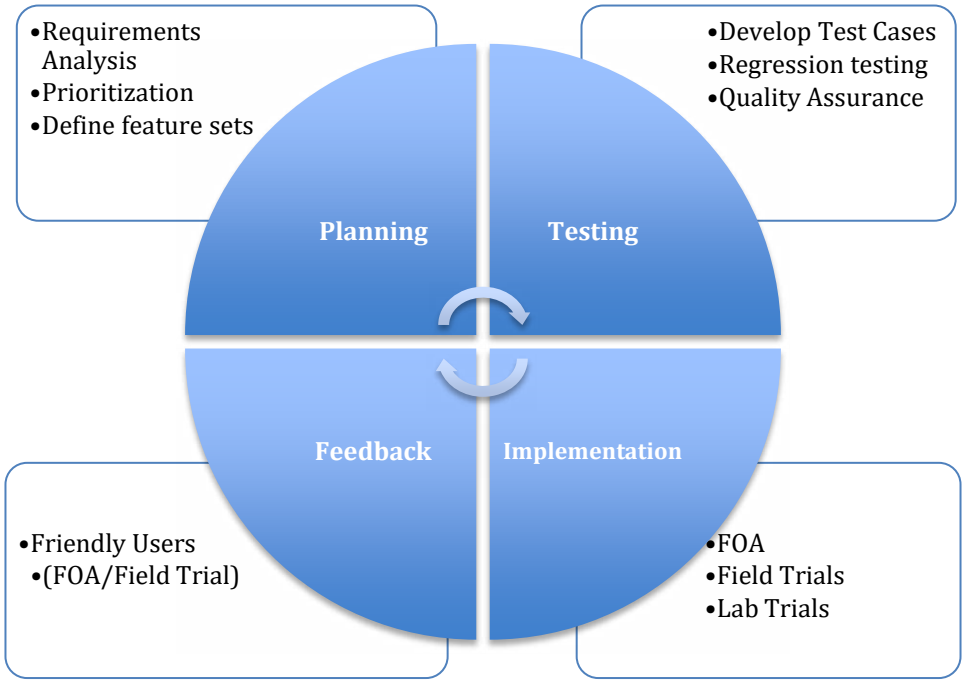


Figure 6: Testing Life Cycle

4.3.2 Device Testing

Commercial network service providers perform several different types of tests on devices they are deploying to ensure that they provide operability within their network and interoperate with their roaming partners, which potentially are operating on different frequencies and/or radio access technologies (RAT). To avoid unnecessary overhead and adversely impacting device availability and/or device interoperability with commercial networks, FirstNet should align with the existing certification processes used by the commercial LTE community. FirstNet should avoid creating a parallel process duplicating already existing test activities and should seek to complement these activities only where and if required.

There are several steps involved in device interoperability and testing in the commercial LTE device eco-system: GCF/PTCRB, Device IOT, regulatory certifications (e.g. FCC part 90), infrastructure vendor IOT and service provider field verification. The service provider does not typically handle the first three steps, but the service provider is presented with the results of the testing. The field verification is service provider specific. A subset of test cases, based on the NPSBN device profile, is used to validate the service provider specific situations. FirstNet should define the NPSBN-specific test scenarios and consider the following testing areas for all devices allowed on the network.

4.3.2.1 Device Conformance Tests

Conformance testing that utilizes independent test organizations such as GCF or the PTCRB should be the first level of testing required. The conformance testing currently evaluates the Device Under Test (DUT) against a validated test platform. These tests evaluate RF, Radio Resource Management, and Protocol Signaling conformance to the 3GPP standard. Additionally, other tests can be added at the request of FirstNet, however, these additions should be minimal as not to require extra cost and time. These types of tests could be additional RF interference testing, or any physical layer test FirstNet may require.

The partners FirstNet utilizes may require optional testing for other networks such as EVDO or HSPA. These tests

should be at the discretion of FirstNet.

4.3.2.2 Device Interoperability Tests

Interoperability between a specific device and multiple infrastructure vendors also must be tested before devices are deployed in a mixed-vendor network. FirstNet should adopt a similar process leveraging interoperability tests performed by vendors and industry associations such as the CTIA LTE IOT Program (CPWG110615-1). Being developed by the CTIA Certification Program Working Group, the LTE IOT Program would be appropriate to consider. This would assure FirstNet that a newly introduced device from a device vendor will interoperate on all of its chosen infrastructure vendors and its commercial roaming partners' networks. Additional tests for multiple users, inter-LTE (other bands) and inter-RAT could also be part of this testing.

4.3.2.3 Device System Tests

Once conformance and interoperability testing is completed, another set of testing is performed before approving a device on the network for operation. The following is an example of the testing that commercial service providers perform on their devices as part of their certification process. Before launching a new device or allowing it to access the network, FirstNet could adopt a similar certification process based on NPBSN defined device testing requirements. It is recommended these testing requirements be included in addition to full lab conformance testing:

- Safe-For-Network Test Plan
- Field Test Plan
- Common Services Test Plan (e.g. SMS, VoLTE, PTT)
- Data Retry Test Plan

4.3.2.4 Device Ancillary Function Tests

Additional device tests could be performed to test the ancillary functions within the device. Other radio access technologies may be implemented within a FirstNet device. If the device utilizes these technologies it is suggested that they are tested. Below is an example list of device ancillary features and their respective testing or test organization:

- Bluetooth - Bluetooth Qualification Requirements[23], established by the Bluetooth Special Interest Group (Bluetooth SIG)
- Wi-Fi – Use Wi-Fi Alliance® test plans[24] to have certified Wi-Fi connectivity
- Universal Integrated Circuit Card (UICC) - USIM/ ISIM applications on the UICC according to 3GPP TS 31.121 and TS 31.124
- Location Based Services – Test to selected LBS specifications, e.g. A-GPS using 3GPP TS 34.171 and 3GPP TS 51.010-1.

4.3.2.5 Requirements for Device and Device Management Testing

[17] Prior to IOT and System-Level testing UEs SHALL have already met 3GPP conformance and certification requirements per an independent conformance testing organization (e.g. PTCRB).

[18] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required Interoperability Testing (e.g. using a subset of applicable test cases from CTIA IOT and UICC

[23] https://www.bluetooth.org/login/default.aspx?ReturnUrl=/technical/qualification/requirements.htm

[24] http://www.wi-fi.org/certification/programs

functional test cases, vendor IOT or similar commercial LTE industry practice).

[19] Prior to operational deployment on the NPSBN, UEs SHALL have passed FirstNet-required UICC functional testing.

4.3.2.6 Device Test Life Cycle

This section is an example of the potential device testing life cycle that could be implemented by FirstNet.

Device - Regulatory, LTE Conformance, Certification …	**FCC Emission Certification – executed at FCC approved labs.**	**3GPP Compliance – executed at approved labs.**	**Other RAT, Compliance (3G, Wi-Fi, etc.) – TBD by FirstNet.**
Device + EPS IOT	**UE + EPS IOT on Network Vendor #1 – TBD by FirstNet.**	**UE + EPS IOT on Network Vendor #2 - TBD by FirstNet**	**….UE + EPS IOT on Network Vendor #n – TBD by FirstNet**
End-to-End Validation Tests	**Safe For Network – executed at approved lab(s)**	**RF, Throughput, other components and accessories – TBD by FirstNet**	**FOA – executed at PS agency TBD by FirstNet**

4.3.3 Infrastructure Testing

Within the LTE network, the system is often split into the Radio Access Network (RAN) and Evolved Packet Core (EPC). Entities outside of the EPC are often considered part of the Packet Data Network (PDN) and can consist of the IP Multimedia Subsystem (IMS), APN servers, Device Management (e.g. OMA DM), IP eXchange (IPX) or essentially any other ancillary systems that are outside of the typical 3GPP LTE diagram [ref 23.401][25]. Each of these systems have specifications or reference implementations within their appropriate Standards Development Organizations (SDOs) such as 3GPP, IETF, and OMA. Due to the vast number of available interfaces and the complexity required to address all of them, the context for this section will be to determine what types of tests FirstNet should require of their vendors.

It is suggested that a set of end-to-end call flows for different scenarios be developed in conjunction with the infrastructure vendors to facilitate better interoperability between the different network elements and the UE. This should be only distributed to infrastructure and trusted UE / chipset vendors under Non Disclosure Agreement (NDA). This will help to drive additional test cases for interoperability.

4.3.3.1 Infrastructure Interface Conformance Tests

These tests will assure that the subsystem under test conforms to the specifications for that equipment. An example of this would be tests developed for the EPC S5 interface to verify conformance to 3GPP specifications. The interfaces are usually divided into the user plane (payload) and control plane (signaling). Both portions of the interface should be tested but typically the primary focus is on the signaling portion within the interface. Some interfaces such as the Uu (air interface) have unique physical layer traits that should be tested in a manner similar to the aforementioned device testing.

4.3.3.2 Infrastructure Interoperability Tests

These tests focus on the evaluation of how different vendor network elements interact with each other. In theory, if the specifications are written perfectly and implemented perfectly, the entire network would be ―plug and play" and interoperability testing (IOT) would not be required. In practice, vendors often interpret specifications differently, are at different versions of the specification, or have implemented proprietary methodologies that may not allow interoperability among vendors. An example of IOT is testing the S6a interface between the MME and HSS from two different vendors.

Interoperability testing allows the network to support multiple vendors between specific interfaces. This would allow FirstNet to leverage competition within the elements of the network and provide more choices for a cost-benefit of features and price among different companies. Several different organizations such as the Multi Service Forum (www.msforum.org) and the Network Vendors Interoperability Test Forum (www.nviot-forum.org) provide a framework for system level IOT on LTE systems and can be leveraged for use by FirstNet to engage in this type of testing.

4.3.3.3 Infrastructure Performance Tests

In order to determine how well a subsystem performs, where the limits are for scaling, and to ensure reliability, it becomes necessary to test to evaluate the peak and loaded performance of the subsystem. This data can be then used to check system reliability, gauge service level agreement (SLA) requirements and load balance the network. An example of testing for this would be simulating several thousand cells on an MME and increasing the calls per second until failure. The Interface Conformance Testing referred to below includes testing of each type of interface deployed per vendor. Subsequent quantities of this same equipment are not tested prior to deployment.

[25] www.3gpp.org/ftp/Specs/html-info/23401.htm

4.3.3.4 Recommendations for Infrastructure Testing

Recommended Requirements

[20] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interface Conformance Testing (e.g. testing S1-MME conformance to 3GPP) on the interfaces specified by FirstNet.

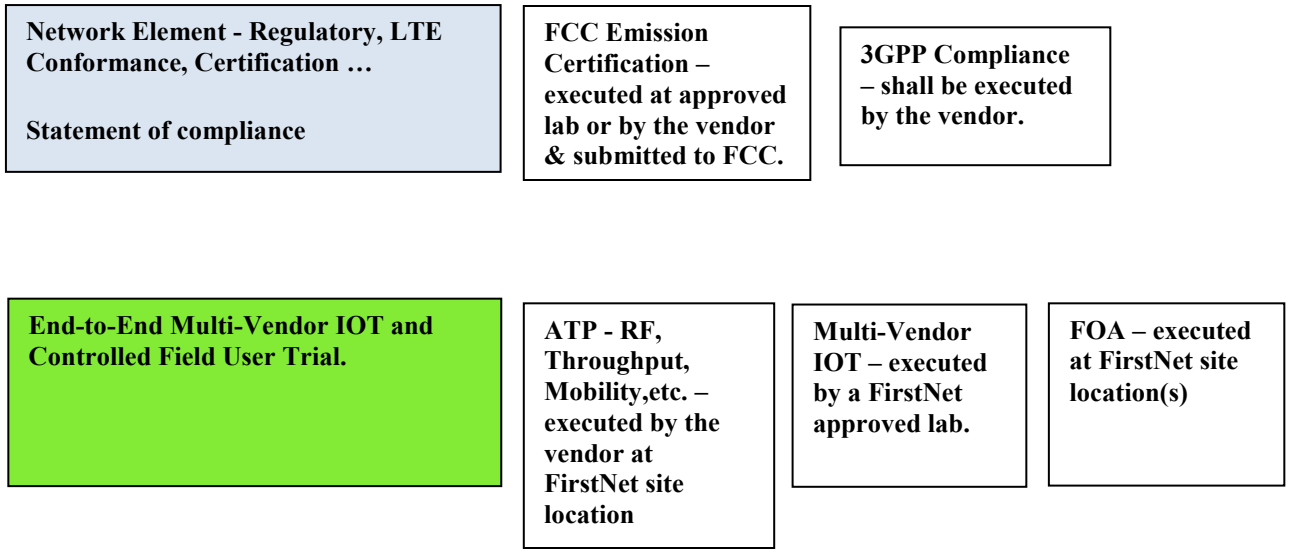
[21] Prior to operational deployment on the NPSBN, infrastructure equipment SHALL have passed FirstNet-required Interoperability Testing at a system level as per the specific IOT requirements for the NPSBN.

Recommended Considerations

(17) Prior to operational deployment on the NPSBN, infrastructure equipment SHOULD have passed FirstNet-required Performance Testing of individual interfaces, nodes and overall system as per the specific performance requirements of the NPSBN.

4.3.3.5 Network & Network Elements Test Life Cycle

This section is an example of the potential infrastructure testing life cycle that could be implemented by FirstNet.



4.3.4 Nationwide Application Testing

Application testing for mobile devices is a complicated task since LTE devices will be in multiple forms such as USB dongles, vehicle modems, and Smartphones. These devices typically run on different operating systems, including Android, Windows 7, Symbian, and iOS. Typically commercial service providers utilize a common connection manager to provide a common user interface across multiple hardware platforms and Operating Systems. For example, a video client on an Android Smartphone and on a Windows 7 embedded modem laptop may operate similarly to the end user but the way they operate to access the QoS to the network is typically operating system and connection manager dependent.

FirstNet may establish specific Application Programming Interface (API) specifications for applications on the network such as Push-To-Talk (PTT). The reason for developing the API specifications is that the PTT application may have specific parameters assigned to it for quality of service (QoS), APN usage, encryption and other application specifications. Application treatment is necessary for FirstNet users; therefore, each FirstNet software application for nationwide use (e.g. PTT, VoLTE, SMS) utilized on the network should pass through a set of tests to ensure it works properly on the device and does not cause unnecessary harm to the network. Most commercial service providers require application certification. FirstNet should employ similar requirements. Testing to the API for security issues may help prevent security issues that could be introduced into the network. Other local jurisdictional software applications are not mandated to pass this testing but it is highly recommended that this type of testing be performed to prevent network issues. FirstNet should consider developing a software applications development guideline, to be used by all software applications deployed on the network, to prevent unintentional network degradation."

4.3.4.1 Recommendations for Nationwide Application Testing

(18) Nationwide applications on the NPSBN SHOULD have passed FirstNet-required security testing to proper security levels (e.g. Criminal Justice Information Services [CJIS]) to ensure protection of FirstNet and public safety information.

4.3.5 System Level Testing

System testing is often called end-to-end testing and typically involves all the components of the network. After all subsystem testing is completed, FirstNet may require that the entire network or major subsystems be run through a series of tests to determine if the functional or systems level requirements for the system have been achieved.

Typically this type of system testing takes place in the form of a First Office Application (FOA) test process. The FOA test case development is a collaboration between the vendor(s) and FirstNet. The FOA performs the following functions:

- Validates that products (equipment & software) meet the test and functional requirements
- Evaluates new features and functionality in customer environment
- Provides essential design feedback between vendor, FirstNet and end customers that will provide quality assurance

4.3.5.1 Recommended Requirements for First Office Application Testing

[22] Infrastructure deployed on the NPSBN SHALL be included in the FirstNet-required FOA process as part of the NPSBN deployment.

4.4 Evolution

4.4.1 Overview

Section 6206 of the Spectrum Act defines FirstNet's duties to include building, deployment, operation and maintenance of the NPSBN. These duties include the need to update and revise established policies established to take into account new and evolving technologies. It is essential that interoperability is maintained as evolution of the NPSBN occurs throughout its lifetime. Wireless service providers typically maintain an organization responsible for establishing network evolution plans and corresponding development and execution strategies. FirstNet will own that responsibility for the NPSBN.

An important element of the policies surrounding development of the NPSBN is establishment of a network evolution framework that will enable public safety officials to leverage the technological advancements that regularly occur in the wireless industry. This provides assurance that first responders will have access to the most advanced communications capabilities possible and that the nationwide public safety wireless broadband network will keep pace with innovations occurring in the private sector. Successful network evolution necessitates striking a suitable balance between the risks, benefits and costs of adopting or not adopting new technologies as technologies and mission requirements evolve. Toward this end, the recommendations provided in this section are intended to help ensure the United States' Emergency Response Providers are able to effectively, and in a cost efficient manner, take advantage of new technologies in a way that best supports public safety mission requirements and sustains nationwide interoperability.

4.4.2 Evolution Scope

The NPSBN evolution plan can be tracked across the layers that comprise the network. Products will clearly fall in a single layer of the network. System features will require coordinated work across multiple layers. The following graphic shows the network layers and the scope of planning for network evolution:

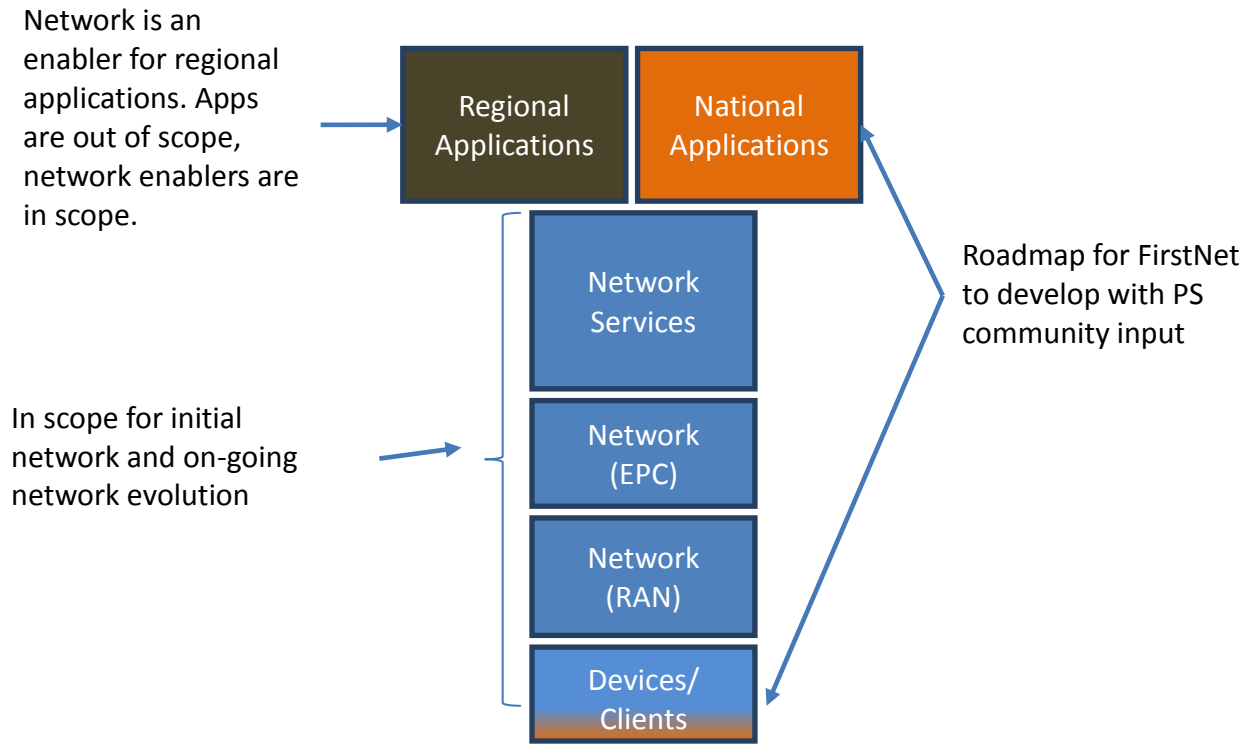


Figure 7: Network Evolution Planning

Planning for coverage, capacity, security and network resilience are additional aspects of the overall plan. Coverage typically impacts only the RAN. Capacity, security and network resilience impact the infrastructure used to provide the network, network services and applications.

4.4.3 Future Applications and Network Services

4.4.3.1 Interoperability with Land Mobile Radio Systems

Networks that provide voice service as an application should provide voice interoperability interfaces to existing agency LMR systems in the area served by the broadband network. Public Safety users on such home or visited networks should be able to call or hail an authoritative dispatch agency or control point using the broadband network subscriber device with microphone and speaker for two-way audio, and talk or be connected to other serving agency voice communications resources. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement.

Recommended Considerations

(19) The NPSBN SHOULD allow for connection and operation of IP-based LMR voice interoperability gateways using open interfaces as they are developed.

4.4.3.2 One-to-Many Communications across All Media – Future Requirement

To ensure nationwide interoperability, the NPSBN should include one-to-many communications capabilities to users within and outside of their jurisdiction (e.g. responding in mutual aid). These communications capabilities should extend from voice, as commonly used in traditional land mobile radio systems, to text messaging, to video, and other forms of data communications. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement.

One-to-many communications could be built utilizing evolved Multimedia Broadcast Multicast Services (eMBMS). eMBMS is standardized in 3GPP and designed to provide efficient downlink (aka, download) delivery of broadcast and multicast services. However, eMBMS is unique in that it requires additional EPS functions and interfaces to support the service and also has impacts to the UE equipment as well. The basic eMBMS service was first introduced in 3GPP Release 9 and has been enhanced in release 10 and 11. As such, eMBMS is a relatively new technology and has not yet been widely deployed in commercial networks. Current target commercial applications include mobile TV and radio broadcasting, as well as file delivery and emergency alerts. Future target public safety applications may include group-oriented multi-media and PTT communications, which could be useful for incident scenarios involving large numbers of NPSBN users who are concentrated in a relatively small geographic area. Obviously a service like eMBMS poses the potential to introduce interoperability issues given its cross-network / UE implications and relative immaturity. We stop short of requiring that eMBMS be implemented in the network, because the delays in availability of final standards and subsequent implementation could unnecessarily delay the construction of the NPSBN.

When eMBMS becomes available and sufficiently capable to support public safety applications, its deployment in the NPSBN should be based on 3GPP standards (R9 or its future successors). Additionally, eMBMS will need to be deployed ubiquitously across the NPSBN in order to provide interoperable services to all NPSBN users. eMBMS would constitute a significant technology enhancement, and as such should be carefully planned and coordinated across the NPSBN. To ease in the transition, infrastructure equipment which is initially deployed into the NPSBN should be upgradable to support eMBMS in the future.

The NPSBN equipment should support eMBMS, when useful and practical, based upon 3GPP standards (current and future evolutions thereof). To the extent that 3GPP standards do not fully specify all interoperable aspects of the eMBMS service (e.g. application APIs and / or interfaces to access the capability), then those aspects should be based on open, consensus-based, non-proprietary, and commercially available standard interfaces.

4.4.4 Evolution of LTE

Driven by needs of the commercial wireless market, evolution of LTE standards proceeds incrementally over a series of releases. Each release of the LTE standard provides a new set of features as required by the market, and a consistent set of specifications from which implementers can build products. New releases of the standards are developed to maintain backward compatibility: LTE user devices built to earlier releases will continue to operate on networks supporting later releases of the standard but may not have the ability to leverage any of the new release's functionality. Development of each release specification occurs incrementally over three distinct stages, allowing different releases to be developed in parallel:

- Stage 1 specifications define the service requirements from the user point of view.
- Stage 2 specifications define an architecture to support the service requirements.
- Stage 3 specifications define an implementation of the architecture by specifying protocols in detail. In addition, specifications related to the testing of each feature are developed in stage 3.

The standardization process ensures development of a consistent set of specifications from which implementers can build products.

4.4.5 Roadmap

To track the evolution of the network, a roadmap for introducing functions into the network is required. The roadmap should track feature availability from vendors, integration testing across vendors, planned market deployment and general availability across the network. The roadmap is used to show services available to end-users in the near term and is used to show need to vendors for longer term items. An open roadmapping process allows both network users and vendors to understand the current high level plan for the network. A key continuing output of the governance of the network is maintenance of a roadmap.

Recommended Considerations

(20) The NPSBN SHOULD be constructed and evolved in adherence to a multi-year roadmap.

This practice is typical of service provider networks and is important to interoperability in that it presents users with foresight of new services and network capabilities as well as plans for elimination of capabilities. This practice is important to the RFP process to allow equipment proposed to be sized for anticipated new features where possible.

4.4.6 Evolution Framework

This section outlines the major considerations that FirstNet should take into account in planning the evolution of the network.

4.4.6.1 Commercial Technology

There is an intrinsic tradeoff between capability/currency and stability/predictability in the adoption of new technology (a risk vs. reward tradeoff). On the one hand, staying current with commercial technology provides public safety with economies of scale, interoperability and best-in-class technology. On the other hand, the standard of reliability and predictability for technology that is used in mission critical situations must be absolutely predictable and reliable. Since the public safety wireless broadband network will employ a commercial technology (LTE), it is important for the network to keep pace with industry advances but in a measured manner. To maximize the stability of the technology, the timing of rollout of each increment (e.g. 3GPP Releases) of technology should lag that of the commercial marketplace, allowing public safety to take advantage of the vast amount of testing performed by commercial service providers. While this may be prudent in order to ensure adequate technology maturity, it may also be dictated by sheer logistics. The challenge here could be to ensure that funding sources are sufficient to keep up with the pace of commercial technology adoption (albeit somewhat phase shifted to allow for

maturation).

The 3GPP specification process for LTE ensures backward compatibility from one LTE release to the next. 3GPP specifications do not require instantaneous synchronization of LTE releases across different networks. Not all portions of the standard are being implemented by vendors and the commercial service providers; furthermore, not all service providers are implementing the standards in exactly the same ways (e.g. some optional features maybe selected by one service provider and not another) or in the same timeframes. Introduction of many capabilities require complex coordination across networks and devices. For example, eMBMS requires changes to the infrastructure (E-UTRAN and Evolved Packet Core) as well as to device chipsets and software. Taking advantage of this new network functionality may require extensive network software upgrades, deployment of new network equipment, and replacement or reprogramming of user devices. FirstNet and public safety should review the specifications in conjunction with vendors and network service providers to determine a feature/function set that best suits public safety.

FirstNet will be responsible for mandating any of the LTE standards as network requirements. FirstNet should, in complementing network evolution, consider existing infrastructure deployments and assimilate them into the evolution of the nationwide network.

Recommended Considerations

(21) Infrastructure equipment procured for the NPSBN SHOULD support backwards compatibility with deployed LTE devices.
(22) Infrastructure equipment in the NPSBN SHOULD be upgradeable to minimally two major 3GPP releases (i.e. n+2, where n is the release available at deployment provided that the equipment does not need to implement a new air interface specification).

4.4.6.2 Compatibility

As commercial technology evolves, new capabilities are introduced. Public safety jurisdictions will need to determine what new capabilities they would leverage for its applications, plan an introduction roadmap, and also ensure that uses of earlier technology is not compromised. This primarily affects four aspects:

Application to Application: This involves ensuring that devices/clients are compatible with other corresponding devices/clients (peer to peer) as well as between the device/client and the network components of the application (e.g. device client to application server such as a database).

Device to Network: This is the area of most scale and individual impact. The evolution plans must consider the useful life / support window for devices on the network and plan the introduction of new technology to accommodate this compatibility window.

Network Element to Network Element: This comes into play as new capabilities are introduced into the network and the updates involve more than one entity in the network and thereby implicitly impact the interfaces between network elements. Introduction of new capabilities (software or hardware) may need to be coordinated to ensure that all impacted elements are properly orchestrated and supported.

Network to Network: There are three main areas of consideration for this.

- Regional operational domain to regional operational domain (IOT and mobility considerations)
- NPSBN to service provider network (primarily roaming considerations)
- NPSBN to Public safety P25/LMR Network

In order for the NPSBN to provide a long-term viable capability, it must evolve along with technology and the commercial industry. In general, standards bodies, such as 3GPP, recognize this as well as the importance of

managing this evolution for users of the network. Interfaces that are extended to users of the network (end-users, application developers, state/agency IT, etc.) must be carefully managed in order to allow users to migrate their dependencies gracefully as the network services evolve over time.

It will be necessary for the equipment comprising the NPSBN to be upgradable to support future features and releases of the applicable standards (e.g. 3GPP). This is common industry-practice in order to ensure cost effective and non-disruptive network evolution. Management of inter-network element (potentially inter-vendor) interfaces is crucial to ensure that the equipment interoperates through successive releases and the evolution of the network.

Recommended Requirements

[23] The equipment comprising the NPSBN SHALL provide backwards compatibility of interfaces, from time of deprecation, for a minimum of two full major release/upgrades of the network. This requirement may be waived (i.e., interface obsolescence accelerated) if FirstNet can ascertain from the user community that there are no dependencies on a given interface.

Recommended Considerations

(23) Hardware and software systems comprising the NPSBN SHOULD support industry practices for management of standard network interfaces from each supplier. These industry practices include formal publication of interface compliance, deprecation of interfaces, support for backwards compatibility and graceful obsolescence of interfaces.

(24) The NPSBN SHOULD support industry practices for life cycle management of interfaces that it exposes to applications or users of the network to ensure backward compatibility for a reasonable interval, using industry-practice interface deprecation and obsolescence methods. The interfaces include, but may not be limited to: Network messaging Protocols, Application Programming Interfaces, Web-based Interfaces, Protocol/Messaging Interfaces, and User Interfaces such as Command Line Interfaces.

4.4.6.3 NG 911 Services

While not completely defined, NG (Next Generation) 9-1-1 services will have an effect on the NPSBN. The following statistics indicate the possible potential to increase network traffic as these devices report public safety events, accidents, injuries or whatever the call might be. Today in the United States, there are approximately 330 million wireless connections, while the U.S. population is slightly more than 312 million. Smartphones are in the hands of about 43% of mobile phone users (62% if you are 25-34) and this number is growing rapidly. Voice communications account for only 1/3 of mobile usage, with the remaining 2/3 of mobile traffic arises from text messaging, applications, video calling, and so forth. Likewise, 32% of adults and 36% of children now live in wireless-only households. In the 9-1-1 arena, 70-80 percent of 9-1-1 calls originate from mobile devices. Consumers rightly and reasonably expect to be able to send data (pictures, video, and text messages) to 9-1-1 call centers. As FirstNet develops the public safety wireless broadband network, it must ensure seamless and secure communications paths exist from the individuals who originate 9-1-1 traffic, through the call/dispatch center, and onto FirstNet's customers in the field. FirstNet must ensure that its network interoperates and interconnects with Next Generation 9-1-1systems to meet the expectations of consumers who request service through 9-1-1. Finally, FirstNet must ensure that its network includes location determination capabilities commensurate with those available to consumers so that its own subscribers can be located when necessary.[26]

4.4.6.4 Coverage

As the network is initially built out, it is expected that it will incrementally expand to increase geographic coverage. As regional networks ~~–~~grow" together, it will be important for the evolution to take into account a cohesive RF plan

[26] The source of the statistics cited above is the 2011 Annual Report of CTIA – The Wireless Association.

and interconnect strategy (e.g. as rural areas add RF coverage, they could be hosted by urban or state-wide networks).

Coverage is complex to engineer in LTE broadband networks since it has many variable components. In general, uplink and downlink user throughputs diminish as one moves from cell center to cell edge (by potentially an order of magnitude or more). User data rates (and, hence, overall capacity) are also affected by adjacent cell activity (interference). This is much different than today's LMR systems, for example. As application types (and priorities) vie for this dynamically varying bandwidth, the network will have to adapt in real time to ensure that the highest priority applications and users are served in the best way possible.

4.4.6.5 Capacity

As usage of the network increases, capacity may need to be enhanced. Capacity enhancements may affect RF planning as well as increase the signaling and bearer traffic loads on core network elements.

Addition of capacity is typically accomplished through the addition of cells (the initial network may be built on a relatively sparse grid). As traffic loading in the network increases, the core network elements and/or links may need additional capacity. Capacity engineering guidelines may be defined and published relative to support for classes of public safety applications and the number of concurrent instances of an application class that can be supported by a given data rate. These would be input to network engineering activities and would help align expectations of network performance overall. However, it is unrealistic to mandate minimum supported rates/performance unilaterally across all networks and locations within the networks. Capacity planning must be coordinated between regional portions of the network and shared national components to ensure that the entire network scales end-to-end.

NOTE: These decisions may be left to regional/local network operation or made in consultation with regional/local authorities.

4.4.6.6 Resiliency

As the NPSBN topologically evolves (sites are added, EPC nodes are added, etc.), overall consideration of network resiliency has to be continually evaluated. This is necessary to ensure that application data centers, EPC nodes, interconnect/backhaul, and RF (where applicable) redundancy is properly engineered and maintained to the necessary standards. Resiliency has to be applied at the regional level to ensure that each such deployment is robust but also must be applied on a national scale for network assets that are truly operated nationwide (e.g. an IP backbone used to interconnect regional deployments). This involves ensuring adequate equipment redundancy to serve expected capacity, geographic redundancy to protect against localized disasters, diversely routed connections, etc. To maximize resiliency, the availability and use of multiple communications technologies and RF bands should be considered.

Recommended Considerations

(25) The EPC equipment in the NPSBN SHOULD support optional local and geographic redundancy.
(26) The equipment in the NPSBN SHOULD support transport redundancy wherever economically feasible (i.e. connections to local switching equipment or WAN connectivity between sites or core locations).

4.5 Handover and Mobility

Handover is a key element of ensuring interoperable communications across the NPSBN. Per 3GPP Standards, handover allows a UE's sessions to be maintained as it traverses parts of the network's coverage area that are served by different cells. Such cells can belong to the same or different PLMNs. In addition, depending on device capabilities, cells may use different radio access technologies (RATs) deployed in different spectrum bands. Seamless service continuity is achieved when the potential interruptions experienced during handover are minimal. Further, for a better user experience, packet loss can be minimized when packets are forwarded from the original cell to the new cell while the handover is being completed.

Roaming refers to the ability of a user device to connect to a network that is not its home network. Such networks may operate in different bands using different technologies. Hence, the user device must also support these technologies to successfully support roaming to the new network. Support for roaming is an essential element of interoperability between disparate systems. It is addressed herein only in the context of roaming between the NPSBN and other networks, such as commercial cellular networks.

4.5.1 Definitions

We define the following terms:

Handover: The process of transferring active voice or data session(s) associated with a wireless device from one cell site to another cell site in the same or a different wireless network while maintaining the device's session(s). To provide a seamless handover experience, the length of time that it takes for the device to switch between the two cell sites (called the interruption time) must be minimized. 3GPP standards do not currently specify the interruption time for intra-LTE handovers.

Roaming: The ability of a wireless user to receive services in a network provided by a different service provider, using a PLMN identity differing from that in the user's home network. This can include mobile as well as Wi-Fi networks. The roaming user is typically charged roaming fees while making use of the roaming network.

4.5.2 Handover

The following schematic will be used to illustrate the handover mechanisms supported by LTE.

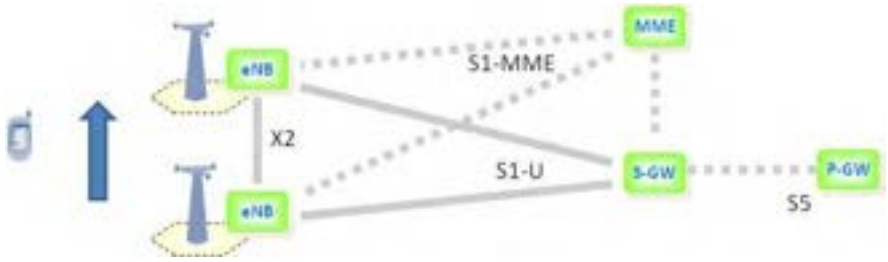


Figure 8: LTE Handover Mechanisms

The following handover scenarios are identified:

- Handover between cells in the NPSBN served by the same MME.
- Handover between cells in the NPSBN served by different MMEs.
- Handover between Band 14 networks with different PLMNs. Such a scenario is representative of a handover between the NPSBN and a commercial provider with whom FirstNet or an opt-out state has a public/private partnership arrangement. Such business arrangements are envisaged by the Spectrum Act,

and supported by RAN sharing features supported by LTE.

Recommended Requirements

[24] The NPSBN SHALL support user mobility across the entire NPSBN (including Opt-out states).
[25] The NPSBN SHALL support S1 and SHALL preferentially support X2 handover between adjacent NPSBN cells (including cells owned by opt-out states) whose proximity supports a handover opportunity.

4.5.2.1 Handover between cells in the NPSBN served by the same MME

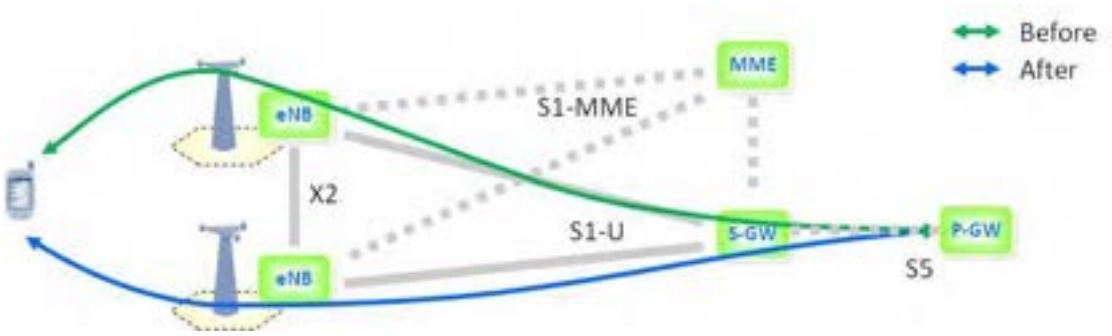


Figure 9: Intra-MME Handover

As shown above, both cells are under the control of a common MME. (As of 3GPP R10, X2-based handovers are only supported between eNBs served by a common MME.) In this scenario, the handover process leverages the X2 interface, supported by supplementary signaling carried over the S1-MME interface. Data forwarding for X2-based handovers is supported via the X2 interface.

During the handover process, Information Elements and signaling messages defined by the 3GPP standards are exchanged between source and target cells over the X2 interface. While X2 handovers use 3GPP's open standard interface, X2 handovers between different vendors' eNBs require inter-vendor testing to ensure interoperability. To reduce the amount of testing required during the early stages of introduction of a new wireless technology, commercial service providers use a practice known as "grouping" – grouping network elements from vendors in their network deployments. The current best practice used by commercial service providers is grouping eNBs from a common vendor into clusters of adjacent cells. These clusters, in turn, are served by a common MME for the purpose of executing X2 handovers and supporting other air interface functions provided over the X2 interface (e.g. scheduling, Inter-Cell Interference Coordination (ICIC), etc.). At the boundaries of these clusters, S1-based handovers are used between eNBs provided by different vendors.

There is on-going work to perform the additional testing required to ensure the interoperability of inter-vendor X2 handovers. As and when commercial service providers start deploying inter-vendor X2 handovers, the NPSBN will also be in a position to support inter-vendor X2 handovers as governed by the NPSBN's network evolution planning. Such an approach will allow the NPSBN to leverage the testing performed by the commercial market. An alternate and potentially resource-intensive approach is for the NPSBN to perform such testing on its own initiative. Until this testing is completed, X2 handovers across vendors cannot be considered interoperable, and hence should not be exclusively required in the NPSBN.

4.5.2.2 Handover between Cells in the NPSBN Served by Different MMEs

When a user/device moves into an adjacent region served by a different MME, the standardized S1 handover mechanism, as shown below, provides seamless mobility.

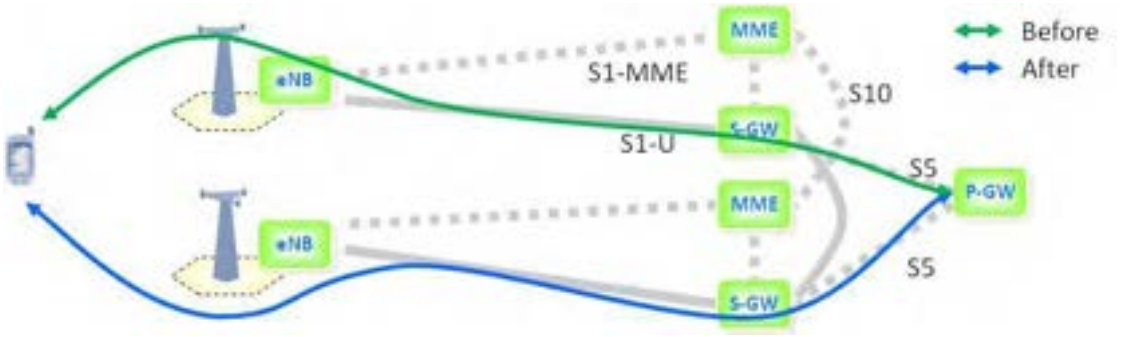


Figure 10: Inter-MME Handover

As illustrated, the handover uses the S1 interface between the source eNB and MME, with the MME coordinating the handover. The MME, in turn, uses the S10 interface to communicate with the MME serving the target eNB to which the user is handed off to. As part of the handover, a new S-GW may be selected as well. In this case packets will be forwarded from the original S-GW to the new S-GW during the handover to minimize packet loss.

4.5.2.3 Handover between Band 14 Networks with Different PLMNs

There may be scenarios in which handover between multiple Band 14 networks, each with a different PLMN ID, is required, e.g. in a public/private partnership with utilities, transportation, or a commercial wireless service provider. The S1 method of handover described in the previous section can also be used to provide handover between Band 14 networks with different PLMN IDs, using the S10 interface between the MMEs in each of the networks. As clarified in 3GPP 23.401, Section 4.2.3, the S10 interface can cross PLMN boundaries. It is expected that the coordination overhead between these networks will be minimal since the number of neighboring cells will be minimal, and primary use may be to handoff to a provider who shares the RAN already.

4.5.3 Roaming from NPSBN onto Commercial Mobile Networks

Sections 6206 and 6211 of the Spectrum Act clearly identify roaming to commercial networks as a key capability required in the NPSBN. It will be especially important during the initial phases of deployment when Band 14 coverage is not yet ubiquitous. Although 3GPP standards support inter-RAT, inter-network handovers between different networks, its implementation would require a significant effort by both the NPSBN and commercial network service providers. For instance, both networks have to open up additional interfaces and provision neighboring cells in each cell of both networks. Currently, this approach is cumbersome and subject to constant churn. One of two alternative approaches should be used:

- Roaming without service continuity, i.e. no seamless service
- Roaming using mobile VPN technology to support session persistence.

FirstNet should also consider Access Network Discovery and Selection Function (ANDSF) as defined in 3GPP 23.402 for roaming to trusted WLAN as alternative to VPNs. ANDSF leverages the LTE credentials for authenticating users, allows seamless handover between LTE and trusted Wi-Fi, and provides similar security as used in LTE. This may allow public safety users to securely and seamlessly roam between NPSBN and their own Wi-Fi networks, e.g. in police and fire stations, without the need for a mobile VPN. The associated cost/benefit should be carefully analyzed on a case by case basis.

4.5.3.1 Roaming Without Service Continuity

To support roaming onto 3GPP and/or 3GPP2 networks, a Band 14 LTE device must accommodate at least one additional 3GPP or 3GPP2 frequency band. If roaming is enabled, the device stays on the NPSBN until the LTE signal becomes insufficient for service, causing the device to go idle and scan for other networks stored in its roaming/white list. If an alternate accessible network is found, the UE will attempt to attach to that network. When

this happens, all active connections are released (dropped), and must be re-established on the new serving network. Note that while roaming onto the commercial network, the user may not have the same capabilities/QoS as experienced on the NPSBN, subject to roaming agreements. While in roaming mode, the device periodically checks for availability of the (home) NPSBN when it is idle as described in 3GPP TS 23.122. Once available, the device moves back to the NPSBN when idle. It is expected that FirstNet will enter in to roaming agreements and associated fees with various commercial service providers. Furthermore, under the terms of the Spectrum Act, FirstNet would make the decision to implement roaming with commercial networks.

The figure below illustrates roaming to a commercial LTE network when home-routed APNs are employed. For this particular case the S6a and S8 interfaces are required between the two networks. An Internetwork Packet Exchange (IPX) provider is expected to be leveraged for the connectivity between the NPSBN and the commercial LTE network for both home-routed and local breakout options as recommended by GSMA PRD IR.88 – LTE Roaming Guidelines.

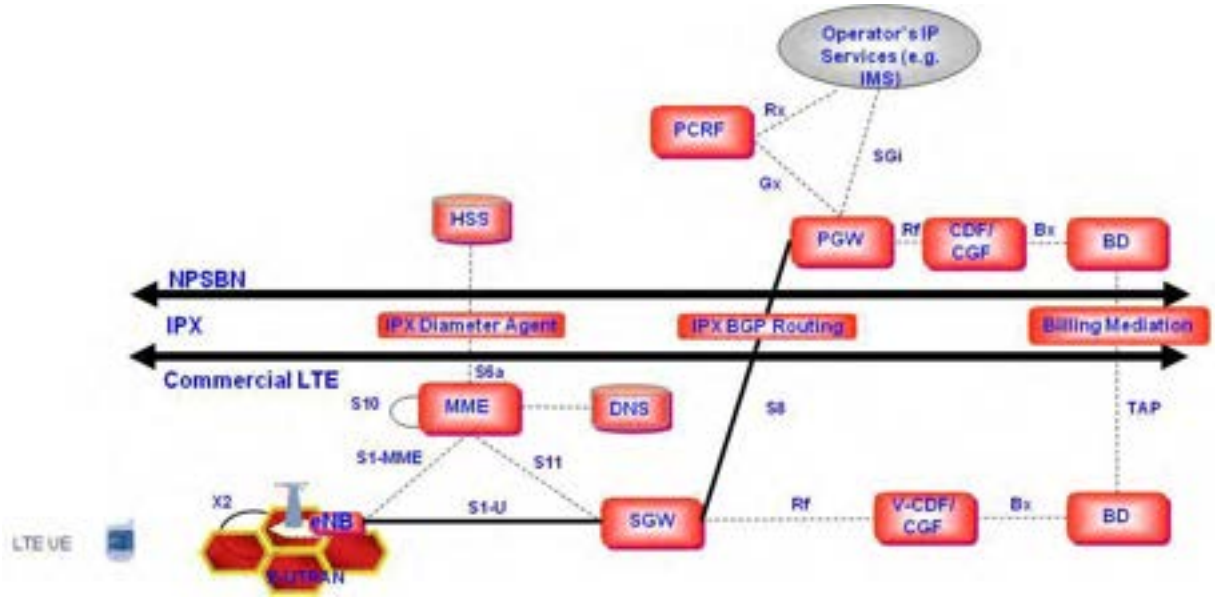


Figure 11: Roaming Using Home-Routed APN

To support local breakout APNs, the S6a and S9 interfaces are required between the two networks as shown in Figure 12.

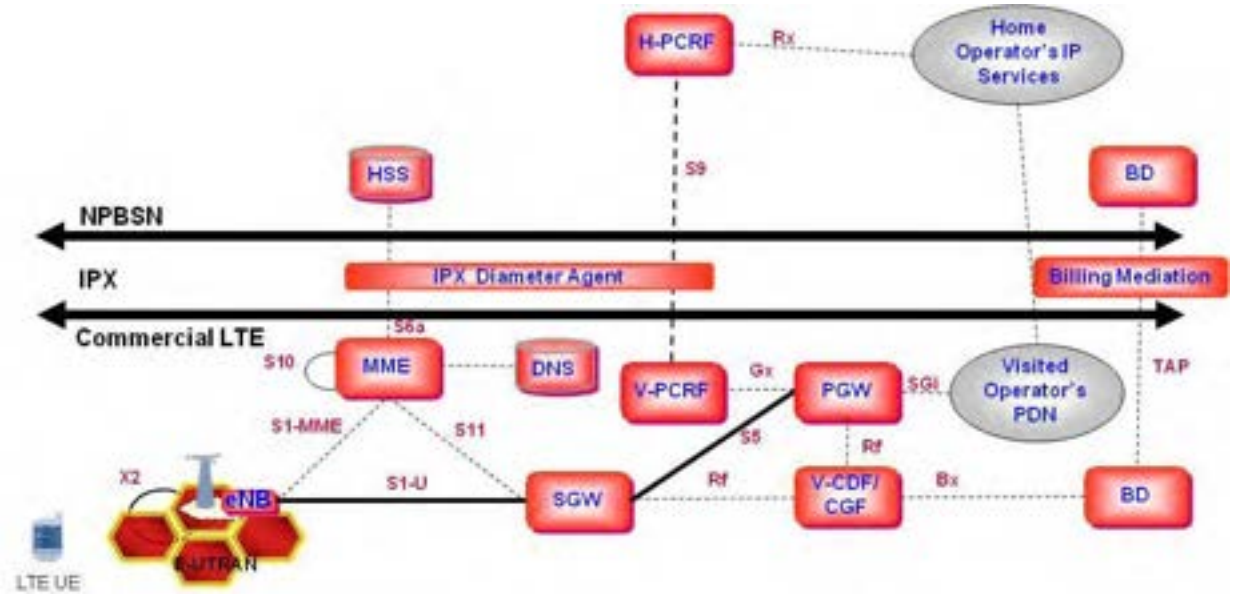


Figure 12: Roaming Using Local Breakout APN

If roaming to 3GPP 2G/3G networks is supported, these networks require the HSS to act as an HLR to the 2G/3G networks to provide an HLR view of subscriber's HSS data as defined in 3GPP TS 23.002. If roaming to 3GPP2 (eHRPD) networks is supported, the HSS needs to support the SWx interface as defined in 3GPP 23.402 to enable an Authentication, Authorization and Accounting (AAA) view of the subscriber's HSS data, e.g. for authentication of the user.

Recommended Requirements

[26] If roaming between the NPSBN and commercial LTE networks is implemented, the NPSBN SHALL follow GSMA PRD IR.88.

[27] If roaming between the NPSBN and commercial 3GPP 2G/3G networks is implemented, the NPSBN SHALL follow 3GPP TS 23.002 to support roaming into 3GPP 2G/3G networks.

[28] If roaming between the NPSBN and commercial 3GPP2 (eHRPD) networks is implemented, the NPSBN SHALL follow 3GPP 23.402 to support roaming into 3GPP2 (eHRPD) networks.

Recommended Considerations

(27) If roaming between the NPSBN and commercial LTE networks is implemented, and IMS is implemented in the NPSBN, the NPSBN SHOULD implement support for IMS while roaming into other LTE PLMNs.

4.5.3.2 Use of Mobile VPN Technology to Provide Session Persistence when Users Roam

Support of session persistence when users roam to other RATs/networks can be provided using mobile VPN solutions. However, the user may experience a short interruption depending on the specific mobile VPN selected. Mobile VPN solutions are currently in use by public safety to, for example, support service continuity between commercial wireless networks and Wi-Fi. In the NPSBN, the choice of whether to use mobile VPNs, and which vendor equipment to use can continue to be made by the individual agencies. Typically this functionality resides in a vehicle laptop or a trunk-mounted vehicle router. To support multiple wireless networks, the mobile VPN device supports a wireless modem for each of the networks it needs to connect to. Each modem has its own wireless subscription with associated monthly fees.

Today, mobile VPN is used with 2G/3G technologies to support best effort services only. When used for guaranteed bit rate services with dedicated LTE bearers, a mobile VPN will be able to maintain service availability, but the alternate access technology may not be able to provide the same quality of experience. For example, if a user is sending real-time video on LTE and loses LTE connectivity, the new network may not have the bandwidth available to continue this video service with the same quality of experience.

Recommended Requirements

[29] The NPSBN SHALL support the use of mobile VPN technology to support mobility between the NPSBN and other networks.

4.6 Grade of Service

An interoperable nationwide broadband network dedicated to public safety must be capable of supporting essential mission critical public safety broadband applications and services on a nationwide basis. A uniform minimum grade of service requirement provides service transparency across various regions and jurisdictions within the NPSBN. Minimum performance requirements also contribute to interoperability by ensuring that mobile users receive consistent service as they move from one area of the network to another, especially in times of emergency.

We acknowledge that budgetary constraints, lack of base station sites (e.g. in remote areas) and other factors may make it difficult to provide a uniform grade of service, especially in the early years of the NPSBN. Because of this constraint, we foresee additional value in providing the NPSBN the ability to offer different Grades of Service in different parts of the country. In such an operating environment, we foresee value in developing a ―common language" to be used across the NPSBN to describe the grade of service provided in different geographic regions. Use of a common language to describe GoS promotes interoperability in the following ways:

- Emergency response planners can take into account the grade of service provided in different geographic regions when developing incident response plans and operating procedures.
- Predictability of service - helping responders know which applications can be supported where. (We note that RF coverage design is not the only factor that influences the data rates users experience. Data rates may be further constrained by policy controls, for example.)

There are additional benefits to providing a common language for grade of service beyond supporting interoperability:

- Common design criteria that can be used for RFPs, helping determining inter-site distances for high-level designs and coverage predictions for RF designs
- Common criteria for measuring grade of service once networks are brought on line

A set of measurable GoS attributes must be established in order to design networks (for purposes of RFPs, for example) and measure performance (for purposes of performance validation, for example). This section discusses GoS attributes used for RAN design. Performance measures used to evaluate a network during acceptance testing or post-launch are also critical. It is recommended that measures and processes be established for both acceptance testing and on-going monitoring of GoS in the NPSBN.

Minimum design requirements adopted for the network must strike a balance between network deployment cost, user quality of experience and network spectral efficiency. In considering these factors, adoption of minimum requirements does not preclude the NPSBN from providing service that exceeds this baseline in different regions.

4.6.1 Coverage Area

A methodology based on the percentage of geographic area covered should be used to determine the degree of coverage within a geographic area. The geographic area is defined as the location (e.g. county, state, city boundary, etc.) within the United States that the NPSBN has targeted for operation. Geographic areas include interior U.S. waterways contained within an area's boundaries. The coverage area is the portion of the Geographic Area where NPSBN service is supported. Different parts of a geographic area may provide different Tiers of Service, as described in Section 4.6.2. As much as possible, coverage areas within a geographic area should be contiguous, thereby maximizing handover opportunities and minimizing service interruptions for mobile users.

In-building coverage, or portability, may be required in densely populated areas or specific venues such as police, fire and EMS stations, hospitals, and other critical infrastructure. On-street coverage, or mobility, may be required in sparsely populated areas. Sparsely populated areas, for example, could be determined on a county by county basis using county-level population densities. It will be important to determine over which portions of a coverage area on-street or in-building coverage is required.

Coverage maps, maps which show pictorially which GoS Tiers (see Section 4.6.2) are supported over a geographic area, are useful tools for operational planning, and hence aid in supporting interoperability. Coverage maps are also useful tools for measuring the progress of network deployment over time and informing the First Responder community of deployment plans.

Recommended Considerations

(28) Coverage maps SHOULD be maintained that show pictorially which GoS Tiers are supported over a geographic area. Detailed maps SHOULD be made available to authorized public safety agencies.
(29) NPSBN coverage maps showing planned future coverage SHOULD be maintained. The maps SHOULD show planned coverage at regular intervals (e.g. quarterly) into the future. These maps SHOULD be made available to authorized public safety agencies.

4.6.2 GoS Tiers

GoS is a multi-dimensional measure of network performance achieved within a Coverage Area. Grade of Service, for example, can be used to describe the minimum expected uplink and downlink data rates and reliability of service throughout a coverage area. The use of different GoS tiers provides the ability for different GoS levels to be supported in different parts of a geographic area based on mission needs, availability of infrastructure and other factors.

To assist public safety practitioners, each GoS Tier should also describe the types of applications that can be supported with clear, common and consistent definitions.

The table below is illustrative of how GoS tiers could be defined.

Tier	Percent Covered	On-Street/ In-Building	Service Probability	Data Rates (kbps)	Applications Supported
1	X%	X	X%	X DL / X UL	X
2					
3					
4					

Recommended Considerations

(30) The NPSBN SHOULD use a set of pre-defined GoS Tiers to provide clear and uniform description of the services of network performance provided within a Coverage Area.
(31) The GoS Tiers SHOULD include the minimum set of GoS Attributes defined in Section 4.6.3.
(32) The expected or actual GoS Tier SHOULD be disclosed to authorized public safety agencies in a geographic region.
(33) Each Coverage Area SHOULD be designed to operate with a defined GoS tier.

4.6.3 GoS Attributes

4.6.3.1 Service Probability

This metric, which can also be called coverage reliability, defines the probability a minimum level of service (e.g. data rate) is met within the coverage area. It quantifies the level of confidence associated with in accessing services within a coverage area. If a service probability is defined as high, then the users will be able to gain and maintain

access to the network more frequently and be refused or have difficulty maintaining service less often.[27]

RF engineering will have a significant impact on the performance of the network and therefore affect service probability. Once a coverage area is specified, cell tower placement, system tuning and ongoing performance maintenance among other factors are critical to achieving high service probability specifications.

Recommended Considerations

(34) Service probability SHOULD be specified for each GoS Tier, in order to specify the quality of the user experience provided by the network.

4.6.3.2 Data Rates

Cell edge data rates, the minimum data rates achieved across a site coverage area with a certain confidence level, are critical design metrics. Cell edge data rates determine the minimum required signal levels that must be supported over a coverage area. The signal levels needed to achieve a target data rate vary across infrastructure and device vendors because of their respective systems' specifications and resource allocation strategy.

Cell edge data rates should be utilized for engineering purposes as they provide a consistent measure of worst-case performance over a coverage area. Minimum data rate is readily measurable, and therefore is a useful statistical tool for quantifying system performance.[28] Due to protocol overhead bits inserted at different layers of the protocol stack, data rates at different reference points in the protocol stack vary. Hence, when minimum data rates are specified, they must also include the protocol layer at which the data rates are to be measured.

Recommended Considerations

(35) The expected minimum uplink (mobile to network) and downlink (network to mobile) rates of data transmission SHOULD be specified for each GoS Tier. The specifications must also include the protocol layer at which the data rates are to be measured.

4.6.3.3 Usage Models

The amount of traffic generated in a coverage area affects interference level, and hence, network performance. Therefore, the NPSBN should be engineered to meet defined Usage Models for each Coverage Area, for example Light, Medium, Heavy or Emergency.

Expected utilization of the network plays a key role in determining the design and effectiveness of the network. A usage model should take into account different customer usage patterns and the data volumes of the applications they will utilize (web browsing, FTP, VoIP, Streaming Video, etc.).

4.6.4 RAN Boundaries & Coordination

[27] RFPs issued by FCC Waiver Recipients have largely specified a 95% probability of service for the Public Safety network. [See LA RICS RFP Addendum 1 Sec. 8.20.5; also City of Mesa, AZ RFP #2010209 Sec. 1.9.1]

[28] RFPs issued by FCC Waiver Recipients have largely specified 768k downlink [system-to-mobile] and 256k uplink [mobile-to-system] for the Public Safety network. [See LA RICS Addendum 8 Section 8.3.3

The handling of RAN boundaries plays a critical role in the design and performance of the NPSBN. As discussed in Section 4.5.2, X2 and S1 handovers provide seamless service. Other handovers, however, can temporarily disrupt service, or, at worst, cause a mobile session to terminate, disrupting service. As a result, handover boundaries must be carefully designed.

Special attention must be paid to boundaries between State Opt-Out RANs and RANs deployed by FirstNet. In addition, interference at such RAN boundaries must be managed. LTE supports multiple capabilities for cell coordination and definition/management of handovers. Whichever approach is selected by FirstNet, it is imperative that it be done in a coordinated manner across the NPSBN. Without coordination, network performance can suffer.

Recommended Considerations

(36) The NPSBN SHOULD implement a scheme for engineering RAN boundaries according to a national cell coordination plan.

4.7 Prioritization and Quality of Service

Prioritization and Quality of Service (QoS) are essential functions in the NPSBN. Prioritization is the network's ability to determine which connections have priority over others. Quality of service is the network's ability to ensure that IP packet flows associated with different applications satisfy performance objectives (e.g. packet loss, delay and throughput) needed for different applications to operate. Thus, prioritization addresses the network connection while QoS addresses the treatment of traffic after the connection is established.

Support of prioritization in the NPSBN must ensure that high priority users can establish connections with higher level of certainty relative to low priority users. In general, priority levels for connections can be defined and assigned based on various criteria (and combinations thereof), including the user's role (or user priority), user application types, or incident type.

Priority access and QoS contribute to interoperability by ensuring that users receive consistent service as they move from one jurisdiction to another, most crucially during times of emergency. Further, priority and QoS help ensure that consistent service is maintained during periods of network congestion. The establishment of a uniform approach to supporting priority access and QoS across the NPSBN that provides service transparency across various regions and jurisdictions within the NPSBN is essential.

In addition, public safety applications[29] such as Computer Aided Dispatch, Incident Command Systems and other applications which exchange information streams over the NPSBN that require QoS support for their proper operation (e.g. real-time video and voice) will require standardized mechanisms to inform the network of the prioritization and QoS attributes of these IP packet streams. Further, these applications will need the ability to modify prioritization and QoS attributes in real-time. In response to an incident, there may be a need to change the priorities of different users, and hence their IP packet flows, to ensure that specific users, devices and applications have appropriate access to network resources. For example, dispatchers might dynamically change specific users' prioritization to ensure that devices and applications have access to network resources during times of congestion.

Hence, applications used by public safety must be able to change priorities and specify QoS treatment of different IP flows using a set of network services that are interoperable across the NPSBN. There are several methods available to public safety applications in order to perform these priority and QoS changes:

- Current standards support use of the 3GPP „Rx" interface to allow an application to convey the responder's priority and provide this information to the NPSBN. A common FirstNet profile detailing usage of the 3GPP „Rx" interface can provide consistent configuration and prioritization across the NPSBN. Given the mature nature of the „Rx" interface standard, it is envisioned as suitable for initial usage by the NPSBN.
- Use of open Application Programming Interface (API) technology and Service Oriented Architecture (SOA) frameworks are accepted industry practices leveraging commercial, open standards for exposing such network features to new and existing applications. Use of open standard APIs such as GSMA's OneAPI with potential extensions for public safety promotes interoperability by providing a stable interface between applications and the underlying LTE network, shielding applications from low-level changes and enhancement of the LTE network as the NPSBN evolves. Leveraging (and, if needed, extending) existing open standard APIs such as GSMA's OneAPI can provide interoperable access to LTE network services.

LTE's prioritization mechanisms provide useful mechanisms for prioritization of public safety traffic. In addressing the topics of prioritization and Quality of Service for the NPSBN, the Interoperability Board reviewed draft work by

[29] Legacy IP-based applications will not support this functionality without additional support functions or enhancement. Standardized mechanisms to inform the network of the prioritization and QoS attributes of these IP packet streams are necessary to ensure that future applications are able to take advantage of these essential prioritization and QoS mechanisms in a common way to ensure interoperability.

the National Public Safety Telecommunications Council (NPSTC) Broadband Working Group's Priority and QoS Task Group.[30] Prior to passage of the Spectrum Act, NPSTC's Priority and QoS Task Group began studying how LTE's standard prioritization and QoS mechanisms could be used to meet public safety's unique mission needs. The Task Group's work continues. We note that some of the mechanisms currently envisioned by the Task Group are currently supported by the LTE standards. Some of the mechanisms, however, will require development of supplemental standards to provide desired functionality (e.g. the creation of Priority and QoS APIs). A description of some of the functional requirements developed by NPSTC is included in Appendix 1.

4.7.1 Profiles: Default Values

3GPP standards define a number of standardized mechanisms to control prioritization and QoS in LTE networks. These mechanisms, tied to the identity of LTE user equipment, utilize a number of parameters which control the way priority and QoS are enforced on a user or class of users, an EPS bearer basis, or multiple EPS bearers per user. These parameters include:

> **Access Class:** Every UE belongs to one or more access classes. A UE's assigned access class is used to determine how often it may attempt to access the network in case of network congestion. Such a form of access control is not generally intended for use under day-to-day network operations: it is expected to be enforced during network congestion or large-scale emergencies (e.g. hurricanes, earthquakes, etc.). A UE's Access Class is stored in its USIM. (See additional background on Access Class in Section 4.7.5.)
>
> **Allocation and Retention Priority (ARP):** The ARP value, assigned per EPS bearer, is used in admission control and is characterized by a priority level, a pre-emption capability and a pre-emption vulnerability. Essentially, this parameter governs if a responder's resource request is granted by the NPSBN. This parameter is also used to determine if a responder's existing application(s) can be pre-empted.
>
> **UE-AMBR:** Defined per UE, the Aggregate Maximum Bit Rate (AMBR) represents the upper limit of aggregate bit rate consumed by a UE for all non-GBR bearers which can be set separately for the uplink and downlink traffic.
>
> **APN-AMBR:** Defined per UE and APN, APN-AMBR represents the upper limit on the aggregate bit rate consumed by a UE for all non-GBR bearers associated with an APN which can be set separately for the uplink and downlink traffic.

Default priority values for these parameters define the day-to-day treatment of user equipment in the NPSBN. Some of these default values (e.g. Access Class) are stored in the user device's USIM. Others are stored in the LTE network's Home Subscriber Server, or Subscriber Profile Repository, and retrieved when a user attaches to the NPSBN.

There are many potential combinations of default values that can be defined for the priority and QoS parameters shown above. To help facilitate operational interoperability, a common set of user profile templates could be used to specify the default values assigned to a user based on the user's day-to-day role. Defining a set of common templates to be used across the NPSBN helps promote operational interoperability by reducing complexity and allowing creation and enforcement of common operating procedures across the NPSBN.

[30] –Priority and QoS in the Nationwide Public Safety Broadband Network," Rev. 1.0, April 17, 2012. (See http://www.npstc.org/download.jsp?tableId=37&column=217&id=2304&file=PriorityAndQoSDefinition_v1_0_clean.pdf)

Recommended Considerations

(37) A set of default QoS profile templates SHOULD be defined for each responder function (e.g. police, fire, EMS) supported by the NPSBN.
(38) Each QoS profile template SHOULD contain a descriptive definition of the responder function and default values for ARP, Access Class, UE-AMBR, and APN-AMBR.
(39) Since the NPSBN could also support secondary users, default QoS profile templates SHOULD be defined for public safety and secondary users.
(40) Every user of the NPSBN (public safety and secondary users) SHOULD be assigned a default prioritization and QoS profile using the set of pre-defined QoS profile templates.
(41) A process SHOULD be established and followed to manage the assignment of templates to users to ensure template assignment rules are uniformly applied for all users using the NPSBN.

4.7.2 Profiles: Dynamic modification

Supporting public safety incident response, planned events, and other situations may require temporary changes to a user‘s default prioritization and QoS treatment. Hence, the NPSBN must allow temporary override of the default profiles.

Recommended Requirements

[30] The NPSBN SHALL provide the ability for national, regional, and local applications to dynamically change a UE‘s prioritization and QoS using the 3GPP ‗Rx‘ interface.

Recommended Considerations

(42) FirstNet SHOULD make an API available to national, regional, and local applications to expose Priority and QoS control.

4.7.3 QoS Class Identifiers (QCIs)

LTE has developed standardized mechanisms for defining the QoS requirements of different IP packet flows. These mechanisms are used by the LTE network, for example, to determine how packets should be scheduled for transmission and how other network resources should be assigned to users to ensure the delay, loss and throughput requirements of the IP flows are met.

3GPP TS 23.203 defines a standardized set of QoS Class Identifiers (QCIs) (shown in the table below). This set of QCIs describes the QoS characteristics of all applications that are currently envisioned to be carried over an LTE network. Use of a common set of QCI definitions across the NPSBN facilitates interoperability by ensuring there is a common way to describe the QoS requirements of all applications which use the NPSBN. Use of the standardized set of QCIs defined in the table below also facilitates roaming onto commercial networks – as these networks also use the same standard definitions of QCI defined in TS 23.203.

Table 4: QoS Class Identifiers (Excerpted from table 6.1.7 of 3GPP 23.203 V9.11)

QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
1	GBR	2	100 ms	10^{-2}	Conversational Voice
2		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3		3	50 ms	10^{-3}	Real Time Gaming
4		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g. www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		9			

Recommended Requirements

[31] The NPSBN SHALL support all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.

[32] QoS mechanisms in the NPSBN SHALL comply with 3GPP TS 23.203.

4.7.4 Preemption

Pre-emption is an essential function in the NPSBN to allow appropriate management of the system resources, especially during emergencies. Usage of all 15 ARP values by the NPSBN is essential to provide sufficient priority differentiation for the default and dynamic priority requirements outlined in this section.

Recommended Requirements

[33] The NPSBN SHALL support the usage of all 15 ARP values defined in 3GPP 23.203.

[34] The NPSBN SHALL support the ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203.

4.7.5 Access Class

Per the 3GPP standards, every UE is assigned to one or more access classes. A UE‘s assigned access class is used to determine how often it may attempt to establish communications with the LTE network. Per 3GPP standards, Access Class Barring was designed to give certain classes of UE preferential access to the system (e.g. police get preferential access over consumer users on a commercial system). The ultimate goal of the capability is to protect against random access channel congestion at a site resulting from an ~~–~~access storm” by many UEs at one time.

Under heavy congestion, it is possible to engage Access Class Barring at a given site. Once engaged, certain classes of UE may be substantially delayed from any communication with the NPSBN. This capability is required in the NPSBN primarily in a public/private partnership arrangement where first responders/secondary users as well as commercial users share the Band 14 spectrum and eNBs. Consequently, UEs homed to the NPSBN must be provisioned with an appropriate access class.

Recommended Requirements

[35] The NPSBN SHALL implement a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2.

4.7.6 IP Network Priority

In order to provide consistent end-to-end treatment of Public Safety traffic, prioritization of NPSBN resources must be provided both over the air as well as within the IP network infrastructure. A traditional practice is to align the priority used by the NPSBN IP network and backhaul technology with the scheduling priority (QoS Class Identifier priority, Section 4.7.3). Failure to align these priorities, for example, may result in low over-the-air packet loss rate, but a high IP transport network packet loss rate. This would create a poor user experience, especially for voice and video applications.

Recommended Requirements

[36] The NPSBN SHALL implement a nationwide scheme for assigning QoS Class Identifier priority to IP network and backhaul priority across the entire NPSBN.

4.7.7 (M)VPN Priority and QoS

Public safety relies on VPN and Mobile VPN technology today to securely transport responder traffic from mobile devices to application servers. For example, secure CJIS queries are encapsulated to provide confidentiality and integrity of the transported citizen information. With (M)VPN technology, a variety of applications (CAD, tactical video, surveillance video, etc.) are typically encapsulated into a single „tunnel". Because LTE technology is expected to greatly expand the number and types of multimedia applications available, either multiple (M)VPN tunnels or multiple application flows encapsulated within a tunnel are needed per user to account for the different types of traffic.

The use of a VPN obscures the source of traffic flowing towards a UE. This creates a problem for an application supporting an Rx interface that is unaware of the VPN. This requires an arbitrating function that is Rx and VPN aware is introduced between the application and the EPC.

Recommended Requirements

[37] The NPSBN SHALL support the use of industry standard VPN and MVPN technology, while providing priority and Quality of Service for encapsulated applications.

4.8 Security

The Spectrum Act §6206(b)(2)(A) provides that one duty of FirstNet is to ensure the safety, security, and resiliency of the NPSBN, including protecting and monitoring the network against cyber attack. It is important to note that providing for cyber security requires addressing two distinct types of threats. First, there is the need to protect the network itself from malicious attacks that aim to hamper or interfere with proper operation of the network. Second there is the need to protect identities and information from compromise. In general, specific cyber security mechanisms are designed to address one or both of these threats.

A complete Information Assurance (IA) framework that addresses cyber security involves not only the technical aspects of the security implementation, but also the policies and procedures that form and direct the operational component of the IA implementation. In the same manner that DHS developed a comprehensive view of interoperability, covering Governance, Standard Operating Procedures, Technology, Training and Exercises and Usage, NIST has developed a holistic approach to IA that provides a comprehensive framework for implementing cyber security systems.[31] Cyber security is a multi-dimensional problem and inherently cyber security mechanisms intersect with interoperability considerations on multiple levels. Full treatment of an IA implementation is beyond the scope of the Interoperability Board. Therefore the requirements and recommendations contained in this section are limited to those that are technical in nature and constitute a minimum interoperable security baseline for the NPSBN.

The NPSBN, the collection of state, local and tribal jurisdictional networks and other networks as depicted in Figure 2, will constitute a multitude of security/information domains. SP 800-27 provides a context for discussing information domains:

> *The term information domain arises from the practice of partitioning information resources according to access control, need, and levels of protection required. Organizations implement specific measures to enforce this partitioning and to provide for the deliberate flow of authorized information between information domains. The boundary of an information domain represents the security perimeter for that domain.*
>
> *An external domain is one that is not under your control. In general, external systems should be considered insecure. Until an external domain has been deemed "trusted," system engineers, architects, and IT specialists should presume the security measures of an external system are different than those of a trusted internal system and design the system security features accordingly.*

Figure 13 illustrates a simplified representation of the of the security domains that the NPSBN will interface to.

[31] NIST Special Publication 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.

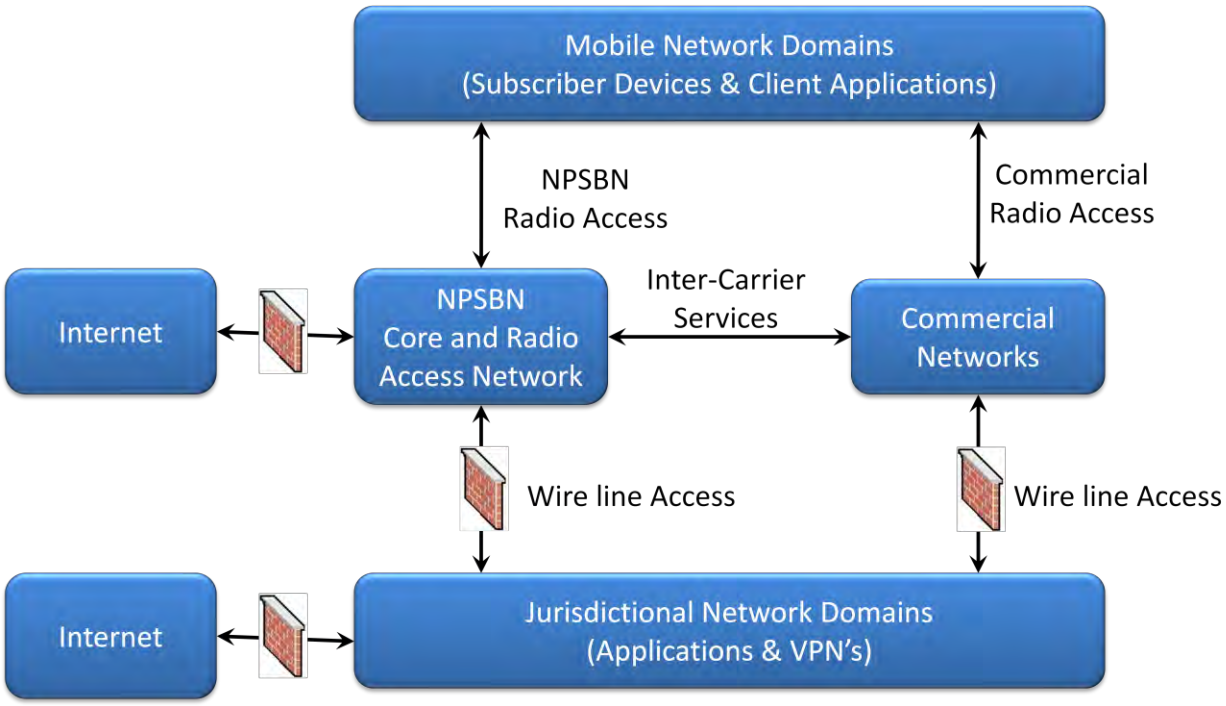


Figure 13: Security Domains

One of the prevailing strategies for dealing with the full spectrum of cyber threats is the implementation of a layered architecture. In SP 800-27 this is described as:

> *Securing information and systems against the full spectrum of threats requires the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. This is due to the highly interactive nature of the various systems and networks, and the fact that any single system cannot be adequately secured unless all interconnecting systems are also secured.*
>
> *By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enable effective protection of information technology for the purpose of achieving mission objectives.*

A layered architecture also serves the purpose of enabling overlay of security implementations that are required by jurisdictional entities in accordance with their individual security policies. For example, as described below, LTE provides a variety of security mechanisms that protect the transport network, including the Radio Access Services and the Internetworking of LTE EPC components. Individual jurisdictions may have a need to augment these security mechanisms in order to provide end-to-end protection of sensitive information, or to provide controlled access to network resources, such as through a secure VPN connection that runs on top of the IP transport services provided by the NPSBN.

As noted earlier, full treatment of cyber security for the NPSBN and associated networks is beyond the scope of the Interoperability Board's charter. Therefore, consistent with the focus on minimum technical requirements for interoperability, and the board's working definition of interoperability, specific requirements and recommendations are limited to the transport network, specifically whose boundaries are defined by 3GPP standards. This focus ensures that two distinct interoperability boundaries are treated, consistent with a multi-vendor environment.

- UE to NPSBN (Core and RAN)

- Connectivity between Core and RAN building blocks

The first case ensures uniform and secure access by UEs to NPSBN transport services, where UEs are provided by multiple vendors that are capable of full mobility across the national footprint of the NPSBN. The second case permits implementation of the NPSBN (Core and RAN) with equipment procured from multiple vendors that possibly exists in one or more security domains. A special case that is provided for are State opt out RANs.

4.8.1 Definitions

When discussing security domains in the broad context, involving both LTE and non-LTE components, the following definitions of domain security are used:

- **Intra-domain security** refers to the system connections and components that exist within a unique combination of network components that constitute a security domain.
- **Inter-domain security** refers to the system connections and components that exist within unique collections of network components, each of which constitute a security domain.

The LTE Evolved Packet System (EPS) composed of the Evolved Packet Core (EPC) and E-UTRAN (RAN) is a flat all-IP architecture with separation of control plane and user plane traffic. Distinct security protection mechanisms are applied to each type of traffic, consistent with the security threats being addressed by each LTE security component. At the discretion of FirstNet, the NPSBN may be implemented with one or more security domains. For example, the NPSBN Core and RAN might exist in a single security domain, and State opt out RANs might exist in their own distinct security domains. The 3GPP Security Architecture in TS 33.210 provides the following definitions for this Inter and Intra domain security. These definitions are applicable to components that are covered by the 3GPP standards and not to the broader security context that involves system elements outside the NPSBN

- **LTE Intra-domain security** refers to the RAN and EPC connections and components that exist under the administrative control of a single administrative authority that can apply a level of security controls and policies across network elements and interfaces within that network.
- **LTE Inter-domain security** refers to the connections that inherently exist between separate network administrative domains. To communicate securely between different administrative domains requires coordination and specification of common security controls and policies to ensure interoperable secure interfaces.

4.8.2 Cyber Security Evolution and Mitigation Strategies

Evolution of the cyber security architecture warrants special attention. Given the prolific deployment of LTE on a worldwide basis, this technology standard will experience unprecedented levels of cyber threats. Cyber threats that are successful against commercial LTE networks may pose a direct threat on the cyber security of the NPSBN, particularly if the NPSBN is implemented with the same vulnerabilities that enabled successful attacks on commercial networks. Given the NPSBN‘s mission, it is prudent to expect that this network will be the subject of direct attacks on a frequent and evolving basis. It is also prudent to expect that evolution of cyber threats will occur at a faster pace than evolution of 3GPP and other standards used in the NPSBN. This is evidenced in commercial markets by the rapid pace at which software vendors distribute security patches compared to the much slower pace at which standards are published and put into practice. For example, LTE releases occur approximately on annual cycles and software security patches to commercial software platforms commonly occur multiple times within a year.

Hence, the Interoperability Board believes it is necessary to afford FirstNet flexibility in addressing rapidly evolving cyber threats, while carefully balancing the somewhat opposing forces of interoperability and security. Therefore, the Interoperability Board recognizes that in response to eminent or present cyber attacks, security

policies, implemented by FirstNet, may dictate the need to depart from security requirements contained in the following sections. The goal is to maintain the highest level of security using commercially available standardized security technologies, consistent with a full Cost/Risk/Vulnerability analysis.

The Interoperability Board also recommends that consistent with layered security architecture, mitigation strategies be employed in the event of major breaches in security. For example, the impact of breach at a lower layer in the security architecture can be mitigated through upper layers, and vice versa. One best practice used in security implementations is the use of bypass mechanisms that permit a compromised security feature to be disabled or bypassed.

Recommended Considerations

(43) The NPSBN security implementation SHOULD include pre-planned bypass mechanisms that have defined security and interoperability implications.

4.8.3 3GPP Security Baseline

As a baseline for its recommendations, the Interoperability Board used the existing report titled "Considerations and Recommendations for Security and Authentication" ("PSAC Report") issued by the Public Safety Advisory Committee (PSAC) commissioned through the Emergency Response Interoperability Center (ERIC) released in May of 2011.[32] While this report was focused on overall network security from a broader perspective, the Interoperability Board felt its work and recommendations were relevant to Interoperability Security.

The Interoperability Board (as well as the PSAC Report) determined that the existing LTE Security Architecture, as outlined in the 3GPP offered the most concise framework around which to develop recommendations. Figure 14 illustrates the LTE Security Architecture.[33] It consists of five security groups. Each security group addresses certain threats and accomplishes certain security objectives:

- (I) Network Access Security – The set of security features that provide users with secure access to services, and which in particular protect against attacks on the (radio) access link.[34]
- (II) Network Domain Security – The set of security features that enable nodes to securely exchange signaling data, user data (between AN and SN and within AN), and protect against attacks on the wire line network.[35]
- (III) User Domain Security – The set of security features that secure access to mobile stations[36]
- (IV) Application Domain Security – The set of security features that enable applications in the user and in the provider domain to securely exchange messages.[37]
- (V) Visibility and Configurability of Security – The set of features that enables the user to determine whether a security feature is in operation or not and whether the use and provision of services should

[32] Emergency Response Interoperability Center, Public Safety Advisory Committee (PSAC), Considerations and Recommendations for Security and Authentication, Security and Authentication Subcommittee Report, May 2011.

[33] 3GPP TS 33.401 V8.7.0 (20-10-04)

[34] 3GPP TS 33.401

[35] 3GPP TS 33.210

[36] 3GPP TS 33.102

[37] 3GPP TS 33.102 and TS 31.111 is an optional feature

depend on the security feature.[38]

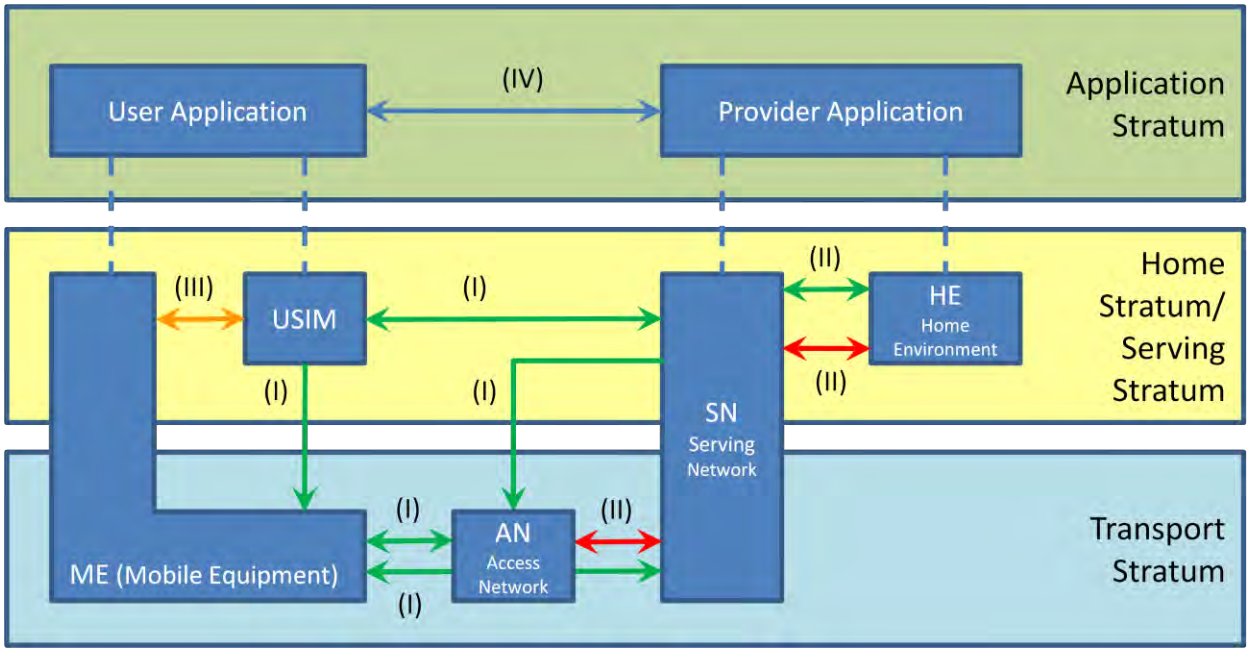


Figure 14: LTE Security Architecture

From this foundation, the Interoperability Board identified the key elements that apply to interoperability.

4.8.3.1 Network Access Security

The UE to EPS interface (radio link) is the most exposed interface and therefore represents heightened security vulnerability. At the same time, a uniform approach to Network Access is required to ensure nationwide mobility, a key component of achieving nationwide interoperability. The 3GPP TS 33.401 Security Architecture shown in Figure 14 defines network access security protocols for UE to RAN and EPC communication, as summarized in Figure 15. In order to ensure interoperable communication between multiple vendors of infrastructure and device equipment, compliance and certification testing to 3GPP security specifications is necessary.

[38] 3GPP TS 33.102 and TS 22.101 is an optional feature

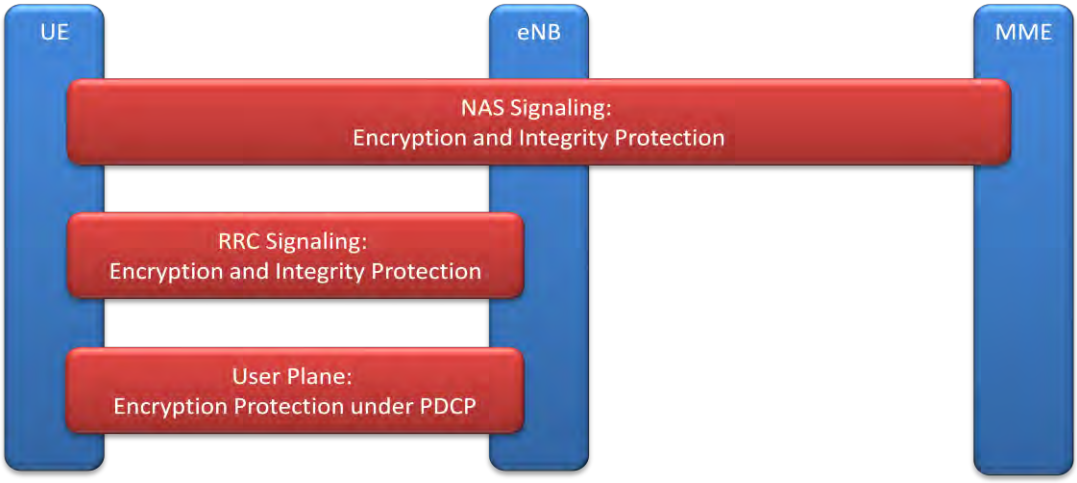


Figure 15: Network Access Security Protocols

Key functions that implement Network Access Security are:

- Access Control – the eNB ensures that only authenticated UEs are permitted to transmit user data to the eNB. UEs that do not successfully authenticate will be prevented from requesting resources from the network to transmit user data.
- Authentication – the UE/USIM and the NPSBN mutually authenticate each other through the use of a cryptographic authentication algorithm that relies on shared key material in both the UE and the HSS. To perform this authentication, both the USIM and the HSS must agree on the same authentication algorithm and share a common set of keys.
- Non-Repudiation – Successful authentication by a UE proves to the LTE network that the device has possession of the physical USIM. USIMs are manufactured utilizing strong physical security techniques to protect the keys used for authentication.
- Data Confidentiality and Privacy – To ensure that information is not disclosed to any unauthorized users via the LTE air interface, both control and user traffic is encrypted utilizing 128-bit AES.
- Data Integrity – 3GPP does not define the use of an integrity algorithm for user data. There are however, integrity algorithms used for all UE-eNB and UE-MME signaling messages.

Interoperable network access security therefore relies on:

- Coordination of the generation of the USIMs with the provisioning and activation of UE devices within the NPSBN HSS is required.
- Enabling HSS to MME signaling so that authentication can be performed. This is required when the UE is attaching to the NPSBN from any eNB in the NPSBN and must also be possible when the UE is roaming to a commercial LTE service provider.
- Enabling the 3GPP defined (but optional per the standard) over the air encryption and integrity features.

Recommended Requirements

[38] The NPSBN SHALL use a nationwide common security profile for user plane and control plane traffic between UEs, eNBs and MMEs, in accordance with 3GPP LTE Network Access Domain protocols. The profile SHALL be based on 3GPP TS 33.401, and will be determined by FirstNet based on a system design and other considerations as it deals with evolving cyber threats. As a minimum, the profile SHALL include specification of ciphering algorithms (for example, use of AES-128 vs. SNOW 3G).

[39] The nationwide common security profile SHALL include ciphering of control plane traffic in order to provide for interoperable cyber protection of the network. Ciphering of user plane traffic is optional and is based on policy decisions that involve FirstNet and user agencies.

[40] To enable interoperable authentication, the USIM and HSS SHALL be capable of supporting the same key derivation functions, such as Milenage per 3GPP TS 35.205, 35.206.

Recommended Considerations

As of the writing of this report, TS 33.401 specifies two different algorithms for 128-bit encryption and message authentication, SNOW 3G and AES.

(44) Equipment used in the NPSBN SHOULD support AES and SNOW 3G algorithms.

The intention is to ensure cryptographically agile deployments that can be reconfigured to utilize an alternative encryption standard (SNOW 3G) if exploits to the 128-bit AES algorithm are discovered.

4.8.3.2 Network Domain Security

The Interoperability Board recommends that FirstNet define the networks, identify the domains of the system, and then apply consistent security policies for interfaces both internal to domains under the control of the NPSBN and also between domains. In the following figure the administrative Domain A controls NE1, NE2 and NE3 and determines the security controls and policies for communication between these network elements. The same is true with the equipment in administrative Domain B for NE4, NE5 and NE6. The interface between these two distinct administrative domains is governed by interoperable security controls and policies. 3GPP TS 33.210 specifies the use of IPSec as the Inter-Domain security control.

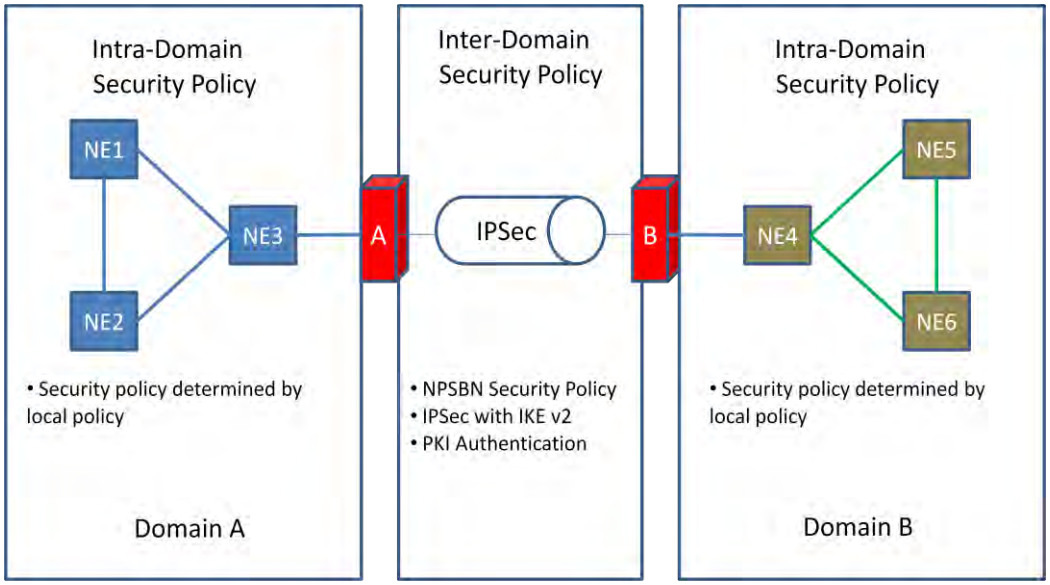


Figure 16: Intra-Domain and Inter-Domain Illustration

Due to the expected threat profile that the NPSBN will be faced with, as noted below, the Interoperability Board recommends that Intra-Domain security controls that are considered optional by 3GPP be required for the NPSBN network deployment. In particular, RANs that rely on long-haul transport networks potentially utilizing commercial and private/government IP wide area network interfaces should secure communication with the EPC utilizing IPSec.

A public key infrastructure is important to provide a scalable key management for the inter-domain interfaces of the NPSBN. To create a PKI, FirstNet would need to establish the policies, procedures, hardware, software and personnel responsible for creation, management, distribution, use, storage, and verification practices of the digital certificates that provide the key material for the network.

Although the Interoperability Board is chartered with identifying Interoperability requirements for the NPSBN, the Interoperability Board recommends that FirstNet undertakes a security risk assessment on the internal interfaces of administrative domains. In particular the Interoperability Board recommends that the NPSBN utilize IPSec to secure network interfaces that cross wide-area network interface such as between the eNB and the EPC.

Figure 2 illustrates the control and user data network interfaces that could potentially fall within the NPSBN. Many of the interfaces that extend from the NPSBN externally will require inter-domain security controls. The Interoperability Board recommends that inter-domain security controls and policies be applied to:

- Ref 3: All S1 interfaces to commercial or PPP networks that transport S1.
- Ref 5: All IP Exchange DCH/FCH, S6a, S8, and S9.
- Ref 6: All IP traffic between the NPSBN and Public Safety Application networks (e.g. public safety agencies).
- Ref 7: Note: IMS specifies the use of IPSec between the UE and the P-CSCF which would occur on top of the Sgi interface within the diagram‘s Ref 14 interface; however the user data plane is not similarly protected by IMS.
- Ref 8: This interface represents an open interface to the Internet. As such, it is assumed that UE‘s who utilize an APN from the Public Internet will be sufficiently hardened.
- Ref 15: LTE mobility interfaces to a Waiver Core.

Recommended Requirements

[41] Network Domain Security SHALL be implemented in accordance with 3GPP TS 33.210, which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).
[42] The NPSBN SHALL comply with TS 33.310 as the authentication framework for Public Key Infrastructure to authenticate these network interfaces.
[43] In order to ensure secure and interoperable interfaces between the NPSBN and external elements (e.g. all SGi, Rx and Srvs services as shown in Figure 2), these interfaces SHALL be protected with a FirstNet-approved security mechanism.

Recommended Considerations

(45) FirstNet SHOULD establish the security controls and policy for inter-domain security and require that all parties (e.g. public safety agencies) who connect to the NPSBN utilize FirstNet-approved cipher suites.
(46) FirstNet SHOULD consider using IPSec interfaces that utilize IKEv2 and utilize PKI to authenticate the peers of the IPSec Security Associations.
(47) When EPS elements are located in trusted locations without wide area communication links between them, the use of network domain security SHOULD be optional.
(48) Network interfaces between domains SHOULD be monitored and intrusion detection/prevention tools SHOULD be deployed.
(49) The developed security mechanisms SHOULD permit local entities to hide the topologies and address spaces of their networks.

4.8.3.3 User Domain Security

Per 3GPP Standards, User Domain Security involves two features:

User-to-USIM authentication:

> *This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret. This security feature is implemented by means of the mechanism described in TS 31.101.*

USIM-Terminal Link

> *This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal. This security feature is implemented by means of the mechanism described in TS 22.022.*

Recommended Requirements

[44] User Domain Security SHALL be implemented in accordance with 3GPP TS 33.102, TS 31.101, and TS 22.022.

4.8.3.4 Application Domain Security

Application Domain Security enables for secure messaging between the USIM and the network (TS 33.102).

> *USIM Application Toolkit, as specified in TS 31.111 [15], provides the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider.*
>
> *Security features for USIM Application Toolkit are implemented by means of the mechanisms described in TS 23.048 [7]. These mechanisms address the security requirements identified in TS 22.048 [16].*

Recommended Requirements

[45] USIM-based applications that require messaging between the USIM and network components SHALL implement Application Domain Security in accordance with 3GPP TS 33.102 and TS 31.111.

4.8.3.5 Visibility and Configurability of Security

In some public safety use cases, it is desirable or even necessary to provide user feedback concerning the security level that a user device is operating (such as Secure or Not Secure). 3GPP LTE standards provide mechanisms for:

- indication of access network encryption: The property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up.
- indication of the level of security: The property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with a lower security level.

The ciphering indicator feature is specified in 3GPP TS 22.101.

3GPP TS133.102 describes configurability as:

> *Configurability is the property that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:*
>
> - Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g. for some events, services or use;
> - Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
> - Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
> - Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

As noted in the ERIC PSAC report, user control of security parameters or their usage is not a generally accepted practice in public safety.

Recommended Requirements

[46] In such cases where visibility is required for devices on the NPSBN, the implementations SHALL comply with 3GPP TS 33.102 and TS 22.101.

4.8.4 Support for Jurisdictional Security Policies

It is essential that the NPSBN support layered security policies that permit jurisdictions to implement their unique security policies, provided that doing so does not compromise the overall security of the NPSBN. Inherently, a jurisdictional security implementation, layered on top of the NPSBN will only be interoperable to users authorized by the jurisdictional security authority. While these layered security mechanisms must be supported, doing so must not be to the detriment of interoperability for users that are not part of that security domain. For example, a jurisdiction may require a particular 2-factor authentication scheme in connection with a secure VPN, based on a commercially available technology. The secure VPN will limit access to a network domain to only authorized users. It is important that this VPN does not have a negative impact to users that are not part of that network domain.

Recommended Considerations

(50) Security mechanisms layered by a jurisdiction on top of the NPSBN SHOULD NOT inhibit interoperability for users visiting from outside of the security domain in which it is implemented.

4.8.5 Roaming

Section 6206(c)(5) of the Spectrum Act permits FirstNet to enter into roaming agreements with commercial network providers. There are many security implications for these roaming agreements that will require robust risk/threat/vulnerability analysis. Of particular concern is the possibility that implementation of these agreements could undermine the security requirements contained in this document. As an example, with 3GPP technologies, a user device is authenticated in the Home Network, and not in the visited network. Therefore, a user device homed to a commercial network would be authenticated by the commercial network and not the NPSBN. If the commercial network operates with an authentication implementation that is less stringent than the NPSBN, a form of ~~–b~~idding-down" of security requirements will occur for users that are homed on a commercial network but operating on the NPSBN RAN and Serving network. FirstNet will need to balance the security requirements with meeting an interoperability goal of this board: to utilize commercially adopted standards.

Recommended Considerations

(51) As FirstNet enters into roaming agreements with commercial partners, security policies SHOULD be implemented that ensure integrity of the NPSBN and that NPSBN security practices are not compromised.

4.8.6 Identity Management and Identity Federation

3GPP standards implement security mechanisms such as authentication from a device perspective, specifically the UE. While these mechanisms are built on sound security principles, they do not support many of the use cases that are important in public safety. There is growing consensus at all levels of government that there is the need to provide authentication not only for user devices, but also for individuals that have access to the NPSBN and for data objects that are accessible by authorized users.

With the proliferation and mobility of devices it will be imperative that the NPSBN ensure that not only are devices authenticated, but that those attempting to use those devices are also authenticated. Because first responders are often asked to support other agencies in mutual aid scenarios, an open, standards based, federated identity management framework is essential to enable users to have interoperable access to applications and data when

authorized to do so. Without an Identity Management framework, application authentication would require unique credentials for each application or applications within an administrative domain and between administrative domains. Such proliferation of access credentials will quickly become a barrier to usability and therefore interoperability if first responders are expected to manage credentials for many different such networks and applications. In such situations it is common for users to replicate the same passwords or write down passwords thereby weakening the security of the system as a whole. We recommend that a framework that retains control of a user's identity by their home agency yet permits these identities to be trusted by applications hosted by other agencies and applications be established. One potential solution has been identified by the Interoperability Board from the DHS/DOJ/HSS National Informational Exchange Model.

Although the NPSBN framework for user identity management provides strong verification of the identity of the user, the information that the user is authorized to access must be determined by the entity that controls the information.

Recommended Considerations

(52) FirstNet SHOULD consider supporting implementation of a national framework for user identity management.

(53) FirstNet SHOULD consider supporting implementation of a national framework for user identity federation to enable user interoperability across administrative domains within the NPSBN, where authorized.

(54) Implementation of the national framework for user identity management and federation SHOULD include a set of guidelines and rules for applications to participate in the national identity management framework.

(55) The agency, organization or entity that utilizes the NPSBN Identity Management framework SHOULD be responsible for enforcing authorization constraints on access to information as per their own security policy.

5 Conclusions

The establishment of minimum technical requirements to ensure a nationwide level of interoperability may seem like a relatively straightforward task. Long Term Evolution (LTE), after all, is based on a set of international standards (3GPP) which are being widely deployed in functioning commercial networks around the world. When one realizes the long term implication of these minimum requirements to the most critical function of government - ensuring the safety of its citizens - the task takes on an added level of gravity and complexity.

This gravity and complexity was noted by Deputy Assistant Secretary Anna Gomez in her remarks before the Interoperability Board on April 23, 2012. In describing the requirements the Interoperability Board was charged with developing, Deputy Assistant Secretary Gomez said —we [NTIA] view [them] as a constitution." This analogy was recalled at numerous times during the Interoperability Board's deliberations as it considered aspects of its work that protected the constituency of the NPSBN (public safety) and the role of those that would govern the NPSBN (FirstNet).

One of the most difficult issues the Interoperability Board dealt with throughout its deliberations was the very thin line that often exists between operability and interoperability. Establishing minimum requirements without a clear understanding of why they are important and how they should be used (operability) is analogous to the United States Constitution without the Federalist Papers. Just as the Federalist Papers are key to the understanding of our Constitution, the informative comments and recommendations made in this document are critical to understanding and implementing the minimum technical requirements for interoperability in a way that ensures operability. While these informative comments and recommendations do not rise to the level of an "incomparable exposition of the Constitution" as historian Richard B. Morris said of the Federalist Papers, the Interoperability Board believes them to be critical to the development of the NPSBN and to its overall success.

In finalizing its set of recommended requirements, the Interoperability Board carefully assessed the sometimes competing components of its relevance tests. There were many discussions around the following topics:

- Whether draft requirements could be considered —minimum technical requirements" as mandated by the Spectrum Act
- Whether draft requirements addressed operability or interoperability
- Whether draft requirements were technical or operational
- Striking a proper balance between granting FirstNet the flexibility it will need to build and maintain the NPSBN while providing the specificity needed to both set a proper course for FirstNet and give the FCC useful tools to determine whether to approve State opt-out plans
- The proper of level of detail to specify requirements in the absence of a nationwide network architecture
- How best to ensure interoperability is maintained as FirstNet and LTE technology evolves

In all its discussions, the Interoperability Board members considered the valuable input it received through the filings in the Docket and its Public Workshop, and the important contributions made by the Consulting Agencies.[39]

The Interoperability Board expresses its gratitude to the Consulting Agencies and subject matter experts that gave many hours of their time to this effort. The Interoperability Board extends a special thanks to the staff of the Public Safety and Homeland Security Bureau of the FCC, without whose support the Interoperability Board could not have accomplished its task. Through this unique collaboration between 15 Interoperability Board members, many SMEs, the Consulting Agencies and the public, the Interoperability Board was able to achieve its legislative mandate in the allotted 60 days. The Interoperability Board is confident that its recommended minimum technical requirements will provide a solid foundation for the successful development of the NPSBN.

[39] Federal Communications Commission Public Notice DA 12-474.

Appendix 1: Public Safety Emergency Services

NPSTC's Priority and QoS Task Group has developed an initial set of functional requirements for a collection of public safety functions, broadly classified in this report as Public Safety Emergency Services.[40] NPSTC continues to develop these key functional requirements for public safety use of the NPSBN to support its mission critical needs. The Interoperability Board recognizes the importance of these functions and the importance of ensuring that these functions eventually are implemented in a fully interoperable manner. Consequently, this informative appendix is included to foster continued dialog by FirstNet, the public safety community and the eco-system that will eventually supply these capabilities to our nation's first responders.

Responder Emergency

Similar to an emergency button on today's LMR radios, activation of this capability provides priority to the first responder's voice service, but also notifies dispatchers and other appropriate personnel of the life-threatening condition. If implemented in the NPSBN at some time in the future, this critical feature must be interoperable across the NPSBN. It is also essential that open standards be developed for this feature and adherence to these standards be validated through testing. For informational purposes, we include the functional requirements developed by NPSTC's Priority and QoS Task Group:

- Provision of standard mechanisms to activate and clear a Responder Emergency by the responder's UE, by a 3rd party via UE (such as a field command tablet), and by 3rd party via a back-end application (such as a dispatch terminal).
- Ability for a responder's agency to define the applications used when one of the agency's responders activates the Responder Emergency capability.
- Activation of the Responder Emergency function provides the highest ARP priority level for emergency applications.
- When activated, Responder Emergency preempts other lower-priority applications on the NPSBN if necessary, in order to obtain resources. Applications used when the Responder Emergency function is activated are prohibited from being preempted.

Immediate Peril

Because all application types (voice, video, data) share a single set of LTE resources, this presents public safety with a new problem not present in LMR systems. A static (default) ordering of application types typically de-prioritizes video and other high-bandwidth applications. This creates a strong lack of flexibility in the framework and likely would prevent video from becoming mission critical. To address these needs, NPSTC's Priority and QoS Task Group defined functional requirements for a prioritization feature which allows a normally de-prioritized application to be ~~"re~~-prioritized" by the NPSBN for a specific first responder, in the event of an *imminent threat to human life*. (We note that this is one example of how such functionality could be implemented. The discussion in this section is not intended to constrain the NPSBN from using other ways of providing this functionality, if needed.)

If such a feature is supported on the NPSBN, it must be interoperable across the NPSBN. Furthermore, open standards must be developed for this feature and adherence to these standards be validated through testing before it is supported on the NPSBN. For informational purposes, we include the functional requirements developed by NPSTC's Priority and QoS Task Group:

- Provision of a standard mechanisms to activate and clear Immediate Peril by the responder's UE, by a third

[40] NPSTC Broadband Working Group – Priority and QoS Task Group – Priority and QoS in the Nationwide Public Safety Broadband Network, Rev 1.0, April 17, 2012.

party via UE (such as a field command tablet), and by a third party via a back-end application (such as a dispatch terminal).

- Ability for the entity initiating the Immediate Peril condition to be able to select the application(s) to receive heightened ARP priority level.
- The ability to utilize both the Responder Emergency and Immediate Peril capabilities from the same entity.

Responder Emergency and Immediate Peril are fundamentally different capabilities and are differentiated by: (1) who chooses the applications to be prioritized, and (2) pre-emption capabilities.

Incident Command System Incident Priority

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

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

Traditionally, incident classification is performed by the Computer Aided Dispatch (CAD) terminal or the ICS COML (communications unit leader) command application. Once this classification is made, an association with NPSBN priority can be made.

Jurisdictional Priority

A first responder‘s jurisdiction is their day-to-day operating area to which they are normally accountable for their function. For example, federal agents may have a jurisdiction which is the entire U.S. territory and local responders may have a jurisdiction the size of a portion of one city. The definition of jurisdiction is relative to the responder‘s agency.

There are a variety of reasons for a responder to exit their jurisdictional area. Examples:

1. Driving to court
2. Training
3. Vehicle maintenance
4. Going home or on vacation

Given these example scenarios, it is possible for a responder‘s UE to unintentionally consume critical resources needed by another jurisdiction. For example, a responder driving to court may stream video from their vehicle in the same cell as a four-alarm fire. Jurisdictional priority is intended to modify (typically lower) a UE‘s ARP priority level when the UE is operating outside its normal jurisdictional area. This prevents accidental use of critical resources in a cell.

However, there are reasons for a responder to operate outside their normal jurisdictional area and still have priority, such as when they provide assistance in a mutual aid incident.

If such a feature is supported on the NPSBN, it must be interoperable across the NPSBN. Further, open standards must be developed for this feature and adherence to these standards be validated through testing before it is

supported on the NPSBN. For informational purposes, we include the functional requirements developed by NPSTC's Priority and QoS Task Group:

- Ability to define and store a jurisdictional area.
- Ability to assign a UE to a home jurisdictional area.
- Ability to allow the local jurisdiction full control of priorities of home and visiting users within the nationwide framework.

Appendix 2: Trusted Delivery Process

The NPSBN is expected to be a highly secure network that will invite cyber attacks because of its highly critical role. A process, defined here as the Trusted Delivery Model, would provide an additional level of scrutiny to help prevent intrusive attacks on the infrastructure elements that would impair or compromise the operation of the NPSBN.

The Trusted Delivery model provides a guideline for applying security assurances to the delivery of network infrastructure hardware, software and firmware. There is not a prescribed standard, but this approach has been adopted by at least one service provider in the United States and one in Canada. The model has four key attributes.

1. An independent assessor is selected by the equipment provider and approved by FirstNet. The assessor does not have to be the same for all equipment.
2. The hardware, software and firmware of the equipment provider are evaluated by the independent assessor. The evaluation identifies security vulnerabilities, malware, Trojans, back door access, and other potentially illicit code. Problematic code is identified to the equipment supplier for corrective action.
3. The hardware, software and firmware delivery method must also be reviewed by the assessor to insure the independently certified equipment is the equipment delivered for installation. This process is also followed for upgrades, maintenance releases and patches.
4. The software and firmware source code should be held in escrow in an independent U. S. based facility to insure a certified copy is always available.

In order to implement this model, these requirements should be included in the Request for Proposal and language inserted in the procurement contract. The Interoperability Board recognizes that this is an emerging area but recommends this as a best practice for the high level of security required for the NPSBN.

Appendix 3: Supporting Agencies and Individuals

The Interoperability Board would like to thank these organizations and individuals for their contributions to the development of the minimum technical requirements recommendations for interoperability. This work could not have been completed without their dedication to the development of the NPSBN.

- **State of Nebraska**
  - Jayne Scofield, IT Administrator
  - Mike Jeffres, Public Safety Systems Manager
  - Matt Schnell, Nebraska Public Power District
- **City of Charlotte**
  - Steve Koman, Public Safety LTE Program Manager
  - Randy Moulton, Chief Security Officer
- **Federal Communications Commission**
  - The staff of the Public Safety and Homeland Security Bureau
  - The staff of the Office of the Managing Director
- **Department of Commerce, National Telecommunications and Information Agency**
  - Regina Harrison
  - Jeffrey Bratcher
  - Dan Phythyon
  - Andrew Thiessen
  - D.J. Atkinson
- **Department of Homeland Security, Office of Emergency Communications**
  - Robert Rhoads
- **National Institute of Standards and Technology**
  - Emil Olbrich
- **Alcatel-Lucent**
  - Wim L. Brouwer
  - Tewfik L. Doumi
- **Harris**
  - Dan Ericson
  - Tom Hengeveld
  - Reid Johnson
  - Patrick Sullivan
- **MetroPCS**
  - Bejoy Pankajakshan

- **Motorola Solutions**
  - Craig Ibbotson
  - Frank Korinek
  - Trent Miller
  - Craig Reilly
  - Gino Scribano
  - Steve Upp

- **Panhandle Wireless**
  - Patrik Ringqvist (Ericsson)
  - G.S. Sickand (Ericsson)

- **Sprint Nextel**
  - Seth Jones
  - Jill Rabach
  - Mark Vangerpen

- **Verizon**
  - David Andersen
  - Bruce Ciotta
  - Renato Delatorre
  - Renitta Burt Geiger

- **Public Workshop Participants**
  - Brian Fontes, CEO, National Emergency Number Association
  - Anna Gomez, Deputy Assistant Secretary for Communications and Information, National Telecommunications and Information Administration
  - Robert LeGrande, Advisor to the City of Baton Rouge, LA
  - Jeff Cohen, Chief Counsel – Law and Policy Director of Government Relations, Association of Public-Safety Communications Officials (APCO)
  - Tom Sorley, Chair, National Public Safety Telecommunications Council (NPSTC) Technology Committee
  - Ajit Kahaduwe, Head of Industry Environment – North America, Nokia Siemens Networks
  - Patrik Ringqvist, Vice President, Wireless Network Solutions, Ericsson
  - Martin Dolly, Lead Member of the Technical Staff, Core Network and Government Regulatory Standards, AT&T
  - Pat Amodio, Chief Engineer, DHS Joint Wireless Program Management Office, U.S. Customs and Border Protection
  - Roger Quayle, Chief Technology Officer and Co-Founder, IPWireless
  - Robert Wilson, Telecommunications Manager, Wyoming Department of Transportation, State of Wyoming
  - Scott C. Somers, Vice Mayor, Mesa City Council, City of Mesa, AZ
  - Mark Adams, Director, Principal Architect, Networks and Communications, Northrop Grumman
  - Thomas Farley, Senior Systems Engineer, Network Centric Systems, Raytheon
  - Matt Schnell, Supervisor of Telecommunications, Nebraska Public Power
  - Mark Althouse, Technical Director – Mobility Mission Management, National Security Administration

Appendix 4: List of Acronyms

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
AMBR	Aggregate Maximum Bit Rate
AN	Access Network
ANDSF	Access Network Discovery and Selection Function
API	Application Programming Interface
APN	Access Point Name
APN-AMBR	APN Aggregate Maximum Bit Rate
ARP	Allocation and Retention Priority
AS	Access Stratum
ATP	Acceptance Test Procedure
BD	Billing Device
BGP	Border Gateway Protocol
CAD	Computer Aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CDF	Charging Data Function
CDMA	Code Division Multiple Access
CGF	Charging Gateway Function
CGW	Charging Gateway
CJIS	Criminal Justice Information Services
COML	Communications Unit Leader
ConnMO	Connection Management Object
CTIA	Cellular Telecommunications Industry Association
DA	Delegated Authority
DHS	Department of Homeland Security
DHS OEC	Department of Homeland and Security Office of Emergency Communications
DCH	Data Clearing House
DL	Downlink
DM	Device Management
DOJ	Department of Justice
DNS	Domain Name System
DoS	Denial of Service
DUT	Device Under Test
EAP	Extensible Authentication Protocol
eHRPD	Enhanced High Rate Packet Data
eMBMS	Evolved Multimedia Broadcast Multicast Service
EMS	Emergency Medical Services
eNB	Evolved Node B
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
EPS	Evolved Packet System
ERIC	Emergency Response Interoperability Center
ESI Net	Emergency Services IP NETwork
ETS	Enabler Test Specifications
E-UTRAN	Evolved Universal Terrestrial Radio Access
EvDO	Evolution Data Optimized
FCC	Federal Communications Commission
FCH	Financial Clearing House
FOA	First Office Application
FTP	File Transfer Protocol
FUMO	Firmware Update Management Object
GBR	Guaranteed Bit Rate

GCF	Global Certification Forum
GoS	Grade of Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GSMA	GSM Association
HE	Home Environment
HLR	Home Location Register
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
IA	Information Assurance
ICIC	Inter-Cell Interference Coordination
ICS	Incident Command System
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IOT	Interoperability Testing
IPX	Internet Packet Exchange
IT	Information Technology
ITU	International Telecommunication Union
LAWMO	Lock and Wipe Management Object
LBS	Location Based Services
LMR	Land Mobile Radio
LTE	Long Term Evolution
MCV	Mission Critical Voice
ME	Mobile Equipment
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MVPN	Mobile Virtual Private Network
NAS	Non Access Stratum
NAT	Network Address Translation
NDA	Non Disclosure Agreement
NENA	National Emergency Number Association
NG	Next Generation
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NPSAN	Nationwide Public Safety Application Network
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OMB	Office of Management and Budget
OS	Operating System
OSINT	Open Source Intelligence
PCRF	Policy Charging and Rules Function
PCS	Personal Communications System
PDN	Packet Data Network
P-GW	Packet Data Gateway
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PPP	Public Private Partnership
PRD	Permanent Reference Document
PSAC	Public Safety Advisory Committee
PSAN	Public Safety Application Network
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTCRB	PCS Type Certification Review Board

PTT	Push To Talk
QCI	QoS Class Identifier
QoS	Quality of Service
RAN	Radio Access Network
RAP	Returned Accounting Procedure
RAT	Radio Access Technology
RFP	Request for Proposal
RMS	Records Management System
RRC	Radio Resource Control
RRM	Radio Resource Management
SAML	Security Assertion Markup Language
SDO	Standards Development Organization
SEG	Security Gateway
S-GW	Serving Gateway
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SN	Serving Network
SOA	Service Oriented Architecture
SRVCC	Single Radio Voice Call Continuity
SUPL	Secure User Plane Location
TAP	Transfer Accounting Procedure
TBD	To Be Determined
UC	Unified Command
UE	User Equipment
UICC	Universal Integrated Chip Card
UL	Uplink
UMTS	Universal Mobile Telecommunications System
USAT	Universal Subscriber identity module Application Toolkit
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
V-CDF	Visited Charging Data Function
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VoLTE	Voice over LTE
VPLMN	Visited Public Land Mobile Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WPS	Wireless Priority Service

Table of Contents

List of Figures

List of Tables

1 Document Overview

This document provides views of the interfaces between the First Responder Network Authority's (FirstNet) Core network and other external networks, including each interface's associated technical description, interface standards, and future interface standards required to meet the Final Operational Capability (FOC) milestones that the Contractor will implement as part of its Nationwide Public Safety Broadband Network (NPSBN) offering.

The document details the external interfaces and their relevant standards and specifications necessary for the implementation of the NPSBN. The following interfaces are:

1. Devices Interface
2. Radio Access Network (RAN) (FirstNet- and State-Deployed RANs) to Core Interface
3. Roaming Interface
4. Mobile Virtual Network Operator (MVNO) Interface (if applicable)
5. Public Switched Telephone Network (PSTN)/Internet Service Provider (ISP) Interface
6. Applications Ecosystem Interface
7. Public Safety Enterprise Network Interface

Each interface is described across five planes—transmission, control, security, user, and management. Each plane is a logical or physical layer associated with the overall network architecture, and each carries a different type of traffic.

1. Transmission Plane is the transmission L1 and L2 physical link and data link
2. Control Plane carries signaling, channel control, and L3 routing traffic
3. Security Plane is security access and egress flow control traffic
4. User Plane carries the network user bearer traffic
5. Management Plane carries administrative and operational traffic

The interface sections within this document utilize the following three system and standard views between FirstNet and other external networks:

- **SV-1** – A systems, components, services interface view identifying all interfaces needed during Initial Operational Capability (IOC) through FOC milestones
- **StdV-1** – A technical standards description of each of the identified interfaces during IOC
- **StdV-2** – A technical standards description of each of the identified additional interfaces required at FOC.

These views are not exhaustive and are used as a guideline for the Contractor to identify all standards that are relevant on an interface. The objective is for the Contractor to utilize standard interfaces.

2 SV-1 NPSBN Interfaces

SV-1 (systems view) provides at a high level the NPSBN and its systems/view interfaces. Interface #1 spans both state and commercial RANs to interoperate with the many different types of devices. Interface #2 is a 3rd Generation Partnership Project (3GPP) Long Term Evolution (LTE) standards-based interface within the network between the Contractor's Core and any RAN. Interfaces #3, #4, and #5 are

3GPP LTE standards-based interfaces with external networks such as MVNOs, roaming partners, and connections for PSTN and ISP access. Interface #6 is with third-party application providers and developers, and interface #7 is with Public Safety Enterprise Networks (PSENs) hosting their local applications and management functions. The interfaces described within this attachment are not an exhaustive list or complete description. Colors are used to identify the organizational owner of a given function:

- **Green** – FirstNet
- **Blue** – PSEN/Local Agency
- **Yellow** – FirstNet Contractor
- **Gray** – Contractor's roaming partners or integrators

The Contractor shall comply with the current or the latest version of the standard specification specified in the tables contained herein.

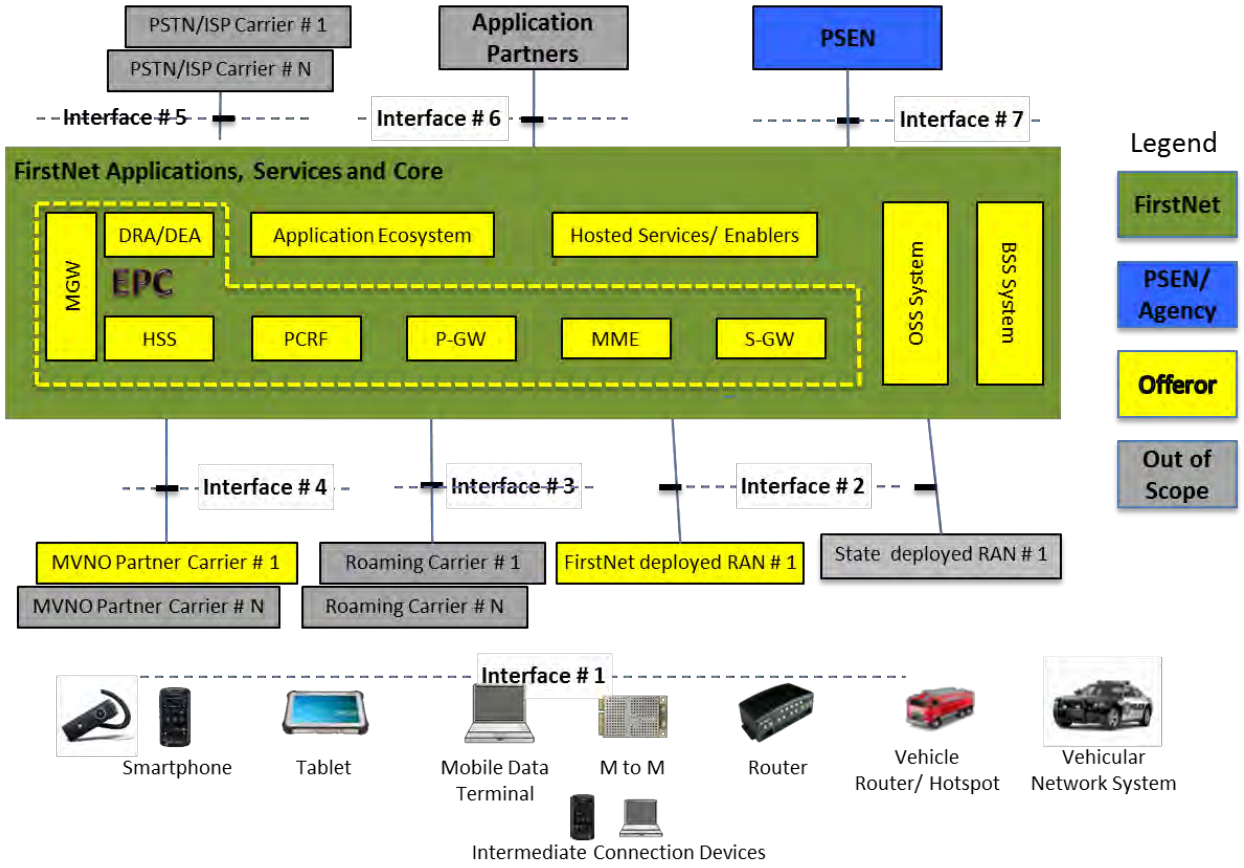


Figure 1 SV-1 NPSBN Interfaces

3 Devices Interface (Interface #1)

The device interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

The devices section covers the system and standard technical views for the interfaces between devices and the NPSBN.

3.1 SV-1 Devices Interface (Interface #1)

The following system view diagram depicts the devices interface.

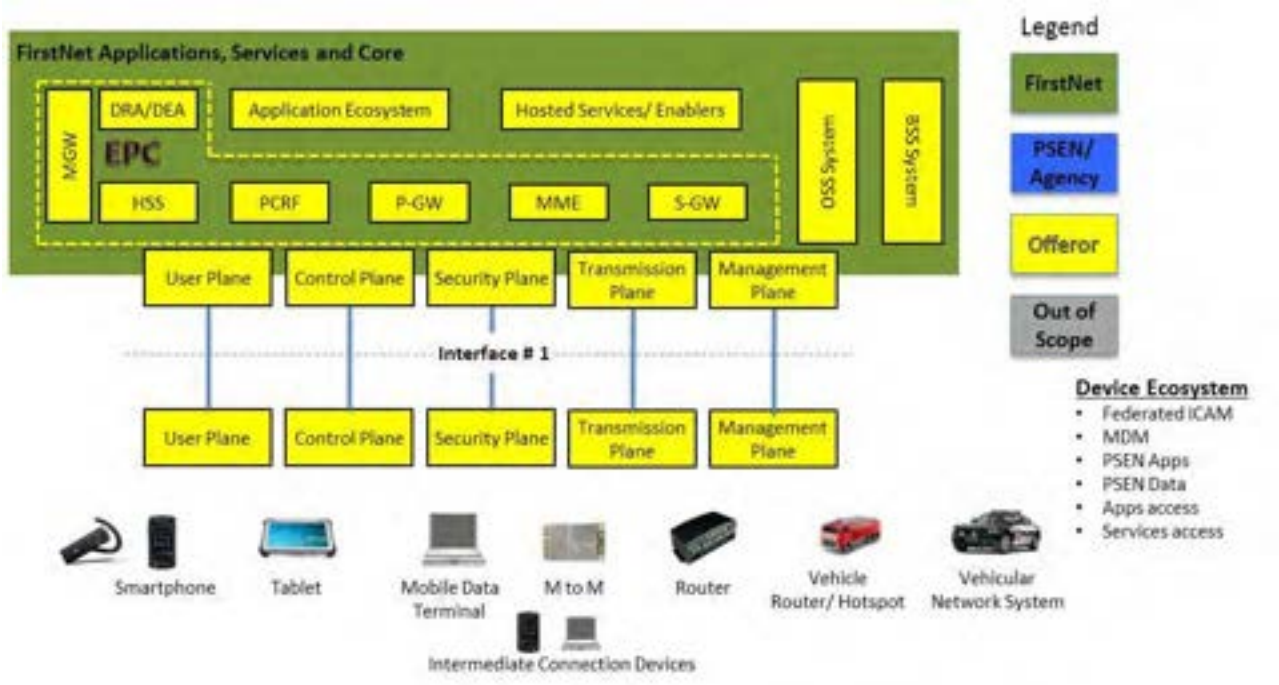


Figure 2 SV-1 Devices

3.2 StdV-1 Devices Interface (Interface #1)

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key device capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

This section also covers the coverage and capacity interfaces between the RAN(s) and Core that are applicable to Vehicular Network Systems (VNS). The VNS platform includes the following major components:

- **In-Vehicle Router** – when the VNS is within terrestrial network coverage
- **Satellite modem and antenna** – once the VNS is fully outside of terrestrial network coverage, it can automatically fall back to the satellite modem from the terrestrial network modem(s)
- **Local Enhanced Node Base (eNodeB) station and antenna** – when the VNS is outside of LTE coverage the VNS can automatically act like a remote base station to other users
- **Local Evolved Packet Core (EPC) elements**

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 1 StdV-1 Devices Interface Specifications.

Table 1 StdV-1 Devices Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User, Control, Security, and Transmission	Uu	Utilize existing LTE standard interfaces including but not limited to 3GPP TS: 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.305, 36.314, 36.321, 36.322, 36.323, 36.331, 33.303, 24.301, 24.334, 24.345, 25.301, 25.144, Utilize existing LTE standard interfaces including but not limited to ETSI TS: 102.671, 102.689, 102.690, 102.921
User	VoLTE	GSMA IR92/94
User	MC-PTT	3GPP TS 22.179, TS 23.779
User	eMBMS	3GPP TS 23.246
User	GSCE/SC-PTM	3GPP TS 22.179 3GPP TS 22.468 3GPP TS 36.890 SC-PTM TS 36.890
User	IOPS	3GPP TS 22.346
User	ProSe PC1: Applications to UE PC3: Core Function to UE PC5: UE - UE	3GPP TS 23.703 3GPP TS 23.713 3GPP TS 23.303 3GPP TS 24.333 3GPP TS 24.334 3GPP TS 36.843 3GPP TS 29.345
User	Locations Services	OMA-SUPL v2.0/3.0 OMA – API http://technical.openmobilealliance.org/Technical/technical-information/oma-api-program/oma-api-inventory GSMA OneAPI – http://www.gsma.com/oneapi/
User	Enhanced Messaging	GSMA RCS 5.x
User	Ethernet	100/1000 Mbps RJ45 (Intermediate cabled connection between router platforms to user devices)
User	Wi-Fi	IEEE 802.11 b/g/n 2.4GHz and 5GHz (Intermediate wireless connection between router and Wi-Fi hotspot platforms to user devices)
User	Bluetooth	Bluetooth 4.0 Low Energy (LE) + Enhanced Data Rate (EDR)
User	Satellite data connection	Industry standard satellite IP data connection (VNS satellite fallback for basic internet connectivity when out of cellular coverage.) (Refer to interface 2 information for satellite transmission connectivity SOW operational mode of the VNS platform)
Management	Device Management	OMA-DM v2.0

3.3 StdV-2 Devices Interface Roadmap

The Contractor shall comply with any future and evolving 3GPP standard interface specification requirements as well as transitioning any proprietary services to an industry standard based solution for any mission-critical service device extensions including:

- **Mission-critical video and data** – Mission-critical video and mission-critical data are 3GPP Release 14 features. Currently, use cases and requirements are being developed. The Contractors need to provide the mission-critical video and data services for the public safety operations. The services should utilize the functions in Group Communication System Enablers (GCSE), Proximity Services (ProSe), and Isolated E-UTRAN Operation for Public Safety (IOPS), and interwork with the Mission-Critical Push-to-Talk (MC-PTT) service.
- **MC-PTT enhancements** – The Contractor needs to incorporate enhanced features specified after 3GPP Release 13, including but not limited to priority, MC-PTT user and group identification, floor control, and group communications and management.
- **Group communications enhancements** – The Contractor needs to incorporate enhanced features specified after 3GPP Release 13, including but not limited to the enhancements to Single Cell Point-to-Multipoint (SC-PTM) transmission and Evolved Multimedia Broadcast Multicast Service (eMBMS) to allow flexible eMBMS bearers establishment, congestion handling, eMBMS roaming, and MC-PTT applications.
- **Proximity service enhancements** – The Contractor needs to incorporate enhanced features specified after 3GPP Release 13, including but not limited to the enhancements to system architecture, direct discovery, direction communication, relay, service authorization, EPC level discovery, LTE-WLAN direct communication, service continuity, and ProSe identity.
- **Location capabilities enhancements for indoor and outdoor emergency communications**

4 RAN to Core Interface (Interface #2)

The RAN to Core interface for both FirstNet-deployed RAN and state-deployed RAN interfaces will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

This section provides three views of the interface between FirstNet's Core network and FirstNet-deployed RANs and state-deployed RANs.

This section covers the system view and the standards technical view for the coverage and capacity interfaces between the RAN(s) and Core that are applicable to both FirstNet and state-deployed RAN states and territories. Element or entity diagrams are logical and FirstNet equipment and responsibilities may be physically located within FirstNet-deployed RAN state borders.

4.1 SV-1 RAN to Core Interface (Interface #2)

The following system view diagram depicts the RAN(s) to Core interface.

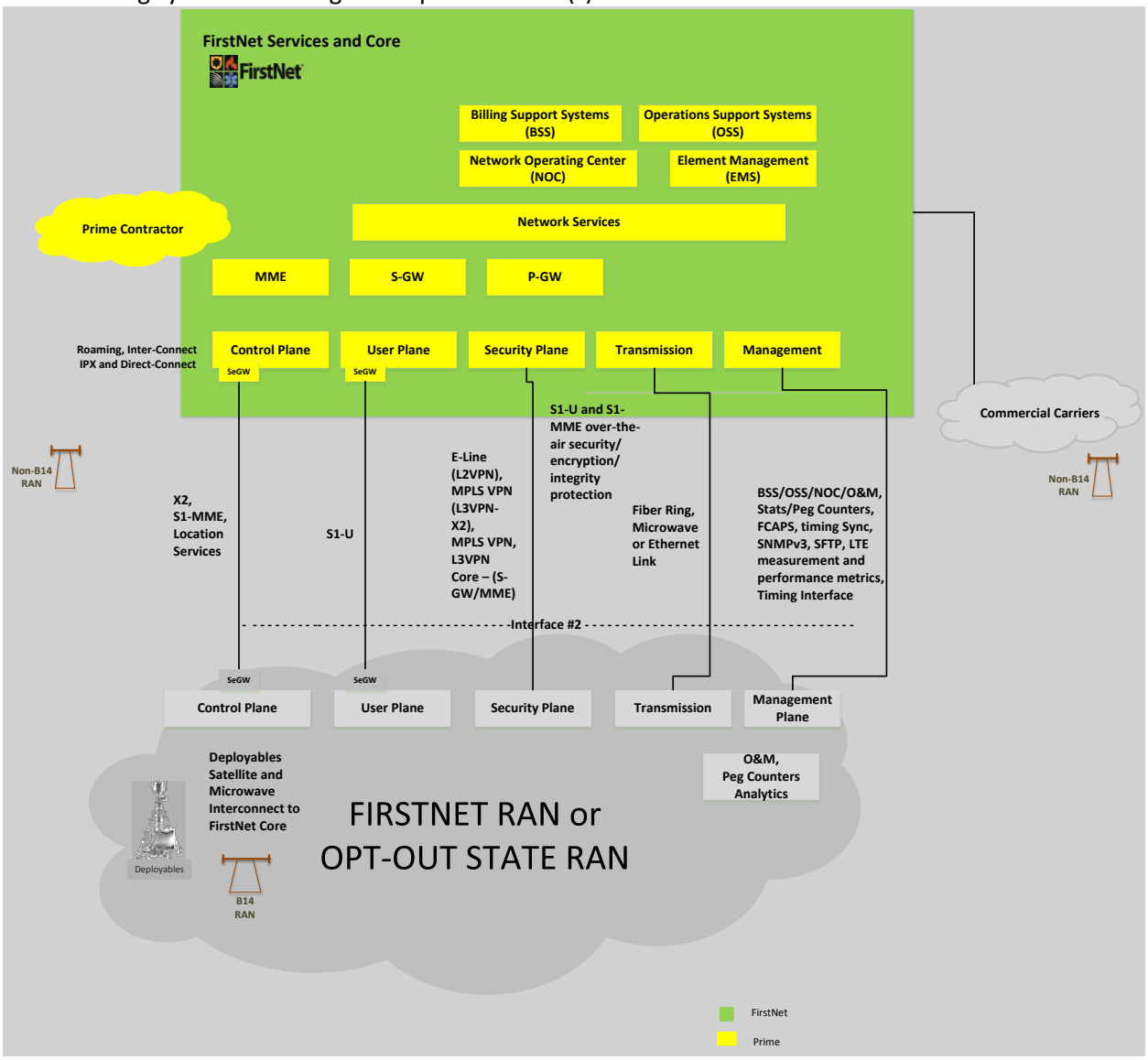


Figure 3 SV-1 RAN(s) to Core

4.2 StdV-1 RAN to Core Interface (Interface #2)

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 2 StdV-1 RAN(s) to Core Interface Specifications. FirstNet foresees that there will be a range of types of deployable units that connect to the FirstNet Core via Interface #2. FirstNet-deployed RANs will utilize, at a minimum, the same interface(s) as the state-deployed RAN interfaces listed below to be fully interoperable.

Table 2 StdV-1 RAN(s) to Core Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S1-U Interface	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.414, 33.210, 33.310 MOCN, GWCN – 3GPP TS 23.236 3GPP TS 23.251
User	Enhanced Messaging Location Services - LTE Positioning Protocol A (LPPa)	3GPP TS 23.271 3GPP TS 36.355 3GPP TS 36.305 3GPP TS36.331 3GPP TS 36.455 3GPP TS 36.355 (LTE positioning protocol) Secure User Plane Location protocol as specified in: OMA-RD-SUPL-V3_0 (requirements) OMA-AD-SUPL-V3 (architecture) OMA-ERELD-SUPL-V3_0 (enablers) OMA-TS-ULP-V3_0 (user plane protocol) Mobile Location Protocol services as specified in: OMA-RD-MLS-V1_3 (requirements) OMA-AD-MLS-V1_3 (architecture) OMA-ERELD-MLP-V3_1 (enablers) OMA-LIF-MLP-V3_3 (mobile location protocol) OMA-TS-LPPe-V1_1 (LPP extensions) User Plane: (For reference only) OMA-TS-LPPe v1.1 OMA-SUPL v1.0, v2.0, v3.0 OMA-SUPCS v1.0
Control	S1-MME Interface X2	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.412, 36.413, 33.210, 33.310 MOCN, GWCN 3GPP TS 23.236 3GPP TS 23.251 3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424
Control	Timing Interface	GPS and external 2.048 MHz synchronization and transmission synchronization. The transmission synchronization includes Synchronous Ethernet (SyncE) from ITU G.8262, and Timing over Packet (IEEE 1588). eICIC, CoMP requires +/- 1.5 to 5 µs. ITU-T G.8272 defines requirements for a Primary Reference Time Clock (PRTC).

Service Area (Plane)	Description	Standard and Source Document
Security	IPSec S1 –U Security/Encryption S1- MME Security/Encryption L3VPN	RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP 3GPP 33.210 3GPP 33.310 Section J, Attachment J-10, Cybersecurity
Transmission	Terrestrial or Deployable Copper, Microwave, Fiber, Satellite utilizing standard IP connectivity to (MME, S/P-GW)	Industry standard best practice
Management	LTE measurements and performance metrics Terrestrial or Deployable Copper, Microwave, Fiber, Satellite utilizing standard IP connectivity to (MME, S/P-GW)	Industry standard best practice
Management	SLA Management Performance and Audit Monitoring LTE measurements and performance metrics	3GPP 36.214, 36.314, 36.133, and 32.425
Management	SLA Management Performance and Audit Monitoring EMS to NMS	Industry standard best practice SNMP v3 – RFC 2571 Architecture for SNMP Frameworks, RFC 3411 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) SFTP

4.3 StdV-2 RAN to Core Interface Roadmap

The RAN to Core interface (Interface #2) at FOC shall be compliant with the then-current 3GPP release standards.

5 Roaming Interface (Interface #3)

The roaming interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

This section defines the system view, functionality, and standards that are expected to be deployed during IOC and available at FOC for the Core network. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

This section provides three views of the interface between FirstNet's Core network and roaming partners.

5.1 SV-1 Roaming Interface (Interface #3)

The following system view diagram depicts the roaming interface.

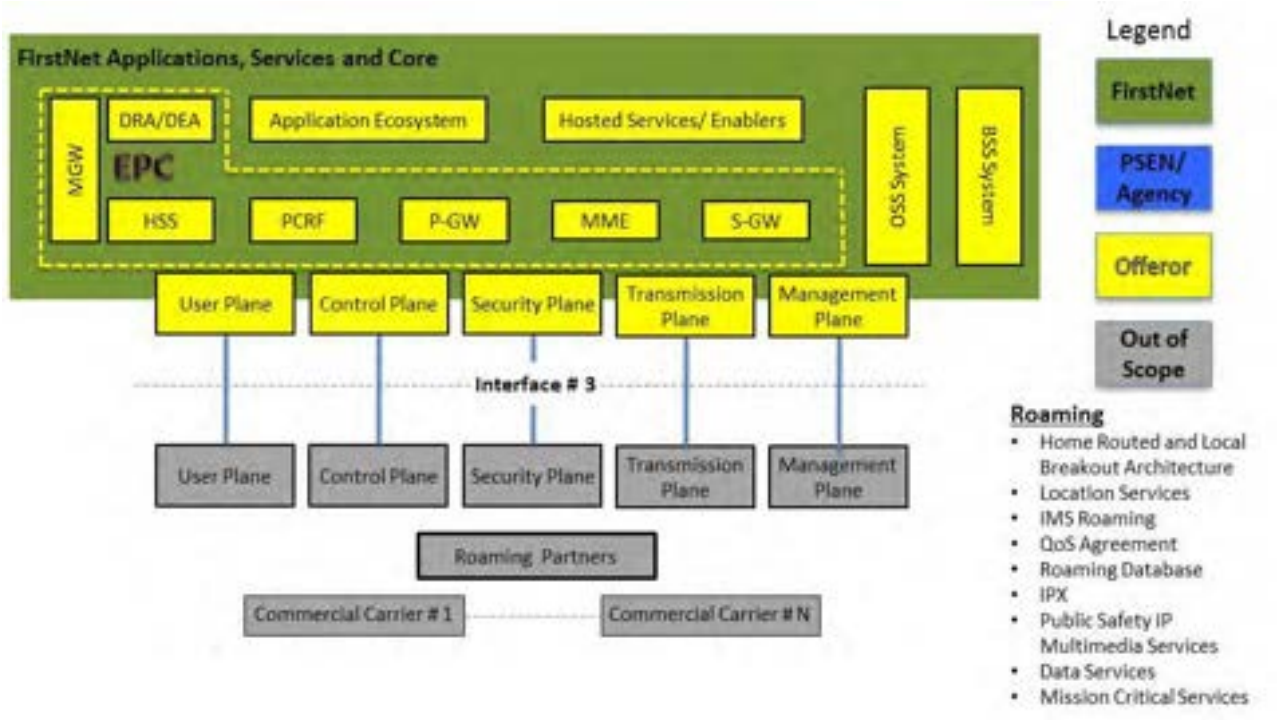


Figure 4 SV-1 Roaming Services

5.2 StdV-1 Roaming Interface (Interface #3)

This section defines system-level interfaces, functionality, and standards that are expected to be deployed during IOC and available at FOC. The focus is on key roaming capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 3 StdV-1 Roaming Interface Specifications.

Table 3 StdV-1 Roaming Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S8, GTPv1-U	3GPP TS 29.281 [32]
User	IMS Emergency Session	3GPP TS 23.167
User	IMS Profile for Voice and SMS	GSMA IR92
User	Locations Services, RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C

Service Area (Plane)	Description	Standard and Source Document
Control	S8, GTPv2-C	3G PP TS 29.274 [31]
Control	Roaming Architecture	GSMA IR.88 [53]
Control	Local Breakout Architecture	GSMA IR.88 [53]
Control	QoS Control	3GPP TS 23.203
Control	DNS/ENUM	3GPP TS 29.303, GSMA PRD IR.67 [52]
Control	DRA/DEA	Defined by IETF RFC 3588 [59] and utilized by GSMA PRD IR.88 [53]
Control	IMS Roaming, Ici/Izi	3GPP TS 29.165 [24], GSMA PRD IR.65
Control	S9	3GPP TS 23.203
Control	Stream Control Transmission Protocol	IETF RFC 4960
Control	S6a, Diameter	3GPP TS 29.272 [30], IETF RFC 3588/3589
Control	Numbering, Addressing, and Identification	3GPP TS 23.003
Control	EPC Architecture	3GPP TS 23.401
Control	Network Architecture	3GPP TS 23.002 [1]
Security	Security Architecture	3GPP TS 33.401 Section J, Attachment J-10, Cybersecurity
Security	IP Network Layer Security	3GPP TS 33.210
Security	IKE with certificates	3GPP TS 33.310
Security	IPSec, Firewall	RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301– Firewall Enhancement Protocol (FEP)
Security	Inter-operator IP Backbone Security Requirements	GSMA IR.77
Security	Roaming Guidelines	GSMA IR.88
Transmission	Standard IP connectivity	Industry standard best practice (Public peering, private peering, or point-to-point connections utilizing Ethernet, VPLS, MPLS, based routing options with appropriate security measures and redundancy to meet objectives)
Transmission	IPX - Secure Roaming / interworking network	GSMA IR.34
Management	Telecommunications Management	3GPP TS 32.101, 3GPP TS 32.102, GSMA IR.88, 3GPP TS 103.260 Part 1 3GPP TS 103.260 Part 2
Management	Roaming Database	GSMA IR.21

Service Area (Plane)	Description	Standard and Source Document
Management	Roaming Charging Aspect	3GPP TS 32.849
Management	Policy and Charging Control	3GPP TS 29.212, 3GPP TS 29.214, 3GPP TS 29.215
Management	SNMP v3 Architecture User-based Security Model for SNMPv3	RFC 2571 RFC 3411 Best practice industry standard specifications for operational support

5.3 StdV-2 Roaming Interface Roadmap

The Contractor shall comply with any future and evolving 3GPP standard interface specification requirements as well as transitioning any proprietary services to an industry standard based solution for any roaming services including these specific public safety mission-critical services:

- Mission-critical video and data
- MC-PTT
- Group communications
- Proximity service
- Enhance location capabilities for indoor and outdoor emergency communications

6 MVNO Interface (Interface #4)

This interface applies if a Contractor proposes to include any MVNO functionality. MVNO interfaces will support existing service, feature, and applications as specified in 3GPP releases in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline for all user, control, security, transmission, and management planes.

When using an MVNO, the NPSBN will maintain its core network, service platforms, Operational Support Systems (OSS), and Business Support Systems (BSS), as well as have its own International Mobile Subscriber Identity (IMSI) codes, Subscriber Identity Module (SIM) cards, numbering space and interconnections. The Contractor will work with FirstNet to innovate and develop leading-edge public safety services and maintain full control of its policies and charging. The NPSBN will interface with its host Mobile Network Operator (MNO) using well-defined standard interfaces in a pseudo-roaming scenario, allowing it to connect to multiple MNOs through the discovery and selection process. In this situation, the NPSBN will operate effectively like a MNO without its own RAN.

6.1 SV-1 MVNO Interface (Interface #4)

The following system view diagram depicts the MVNO interface.

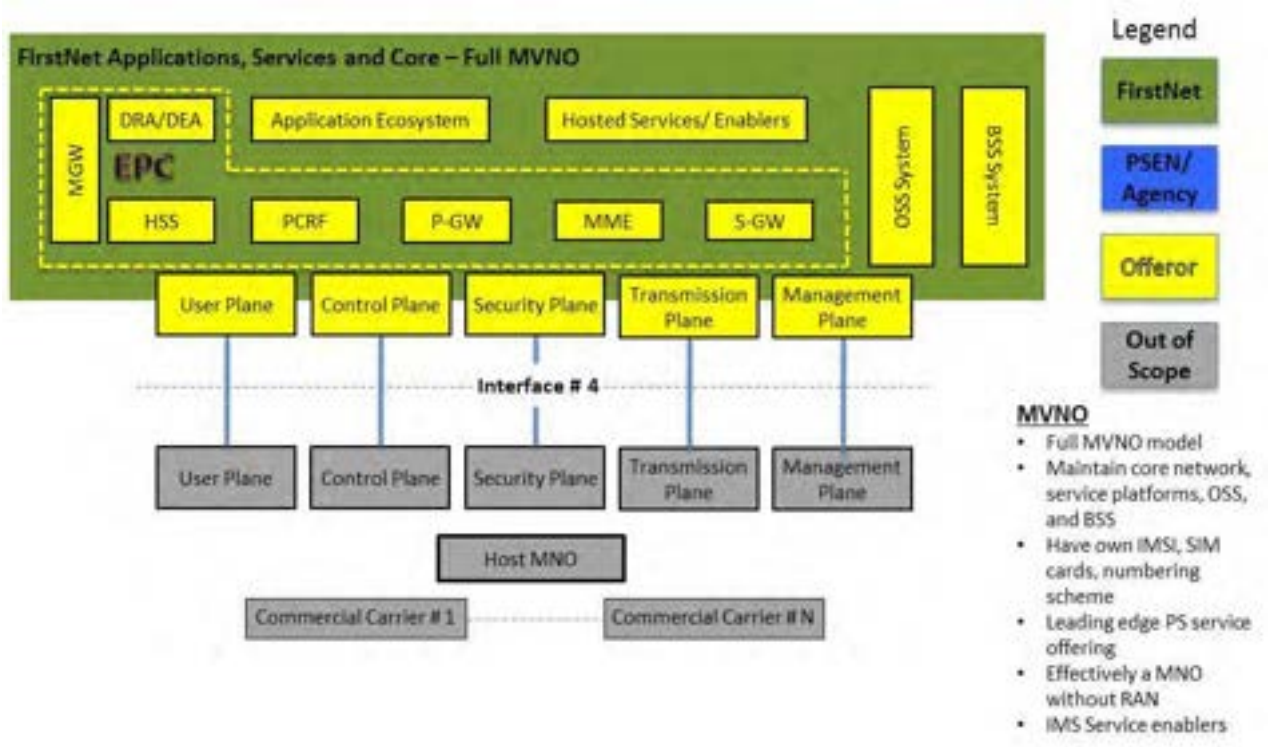


Figure 5 SV-1 MVNO

6.2 StdV-1 MVNO Interface (Interface #4)

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in MVNO Interface Specifications in Table 4 StdV-1 MVNO Interface Specifications. MVNO interfaces will utilize existing service, feature and application interfaces as specified in up to and including 3GPP Releases 13 in accordance with IOC/FOC for all user, control, security, transmission, and management planes.

This section defines system level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key MVNO capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

Table 4 StdV-1 MVNO Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S5/S8, GTPv1-U	3GPP TS 29.281
User	S1-U Interface	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.414, 33.210, 33.310 MOCN, GWCN 3GPP TS 23.236 3GPP TS 23.251

Service Area (Plane)	Description	Standard and Source Document
User	IMS Profile for Voice and SMS	GSMA IR92
User	Locations Services, RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
Control	S1-MME Interface X-2	3GPP TS 23.122, 24.301, 36.410, 36.411, 36.412, 36.413, 33.210, 33.310 MOCN, GWCN 3GPP TS 23.236 3GPP TS 23.251 3GPP TS 36.420, 36.421, 36.422, 36.423, 36.424
Control	Roaming Architecture	GSMA IR.88
Control	Local Breakout Architecture	GSMA IR.88
Control	QoS Control	3GPP TS 23.203
Control	DNS/ENUM	3GPP TS 29.303, GSMA PRD IR.67
Control	DRA/DEA	defined by IETF RFC 3588 and utilized by GSMA PRD IR.88,
Control	IMS Roaming, Ici/Izi	3GPP TS 29.165, GSMA PRD IR.65
Control	S9	3GPP TS 23.203
Control	Stream Control Transmission Protocol	IETF RFC 4960
Control	S6a, Diameter	3GPP TS 29.272, IETF RFC 3588/3589

6.3 StdV-2 MVNO Interface Roadmap

The Contractor shall comply with the mandatory standards interface specification requirements for the full MVNO model in providing mission-critical services, including:

- Mission-critical video and data
- MC-PTT
- Group communications
- Proximity service
- Enhance location capabilities for indoor and outdoor emergency communications

7 PSTN/ISP Interface (Interface #5)

The PSTN/ISP interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

7.1 SV-1 PSTN/ISP Interface (Interface #5)

The following system view diagram depicts the PSTN/ISP interface.

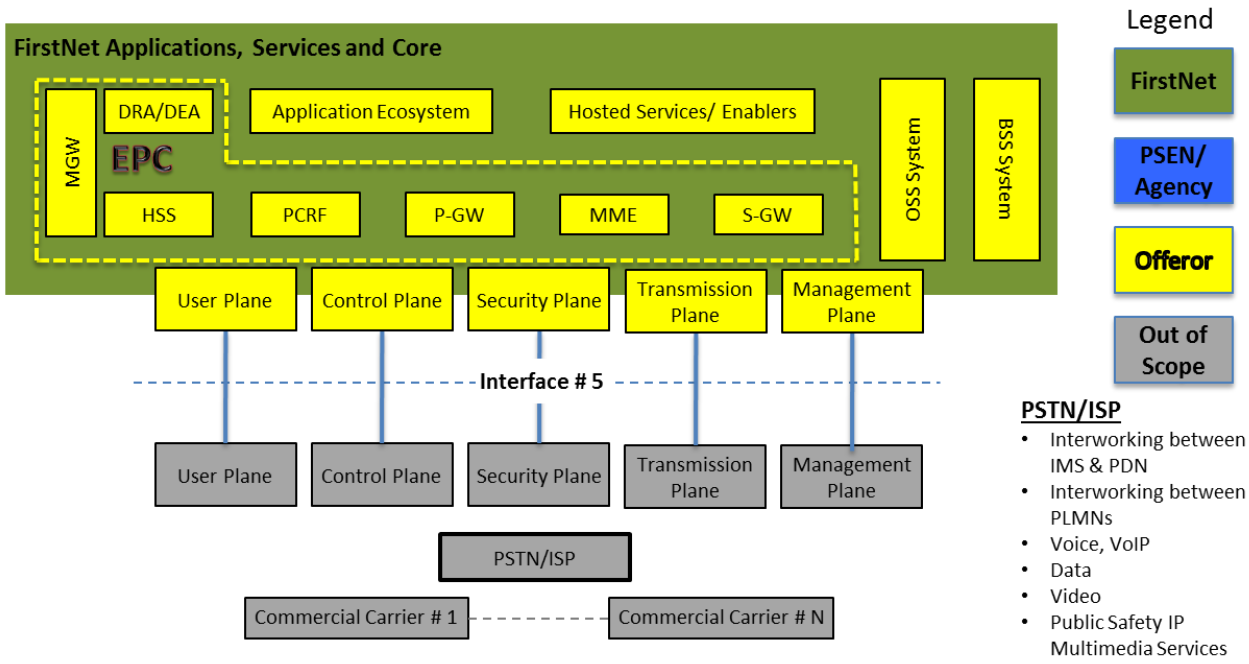


Figure 6 SV-1 PSTN/ISP

7.2 StdV-1 PSTN/ISP Interface (Interface #5)

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key PSTN/ISP interfaces that may not be available at IOC but are expected to be operational at FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 5 StdV-1 PSTN/ISP Interface Specifications.

Table 5 StdV-1 PSTN/ISP Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	S14 – ANDSF	3GPP TS 24.312
User	SGi – Interworking between PLMN supporting PDN	3GPP TS 29.061
User	Pulse code modulation (PCM)	ITU-T Recommendation G.711
User	Packet switched conversational multimedia	3GPP TS 26.235
User	Mb – Interworking between the IMS and IP networks	3GPP TS 29.162

Service Area (Plane)	Description	Standard and Source Document
Control	Mb – Interworking between the IMS and IP networks	3GPP TS 29.162
Control	SIGTRAN	IETF RFC 2719
Control	Stream Control Transmission Protocol (SCTP)	IETF RFC 2960
Security	Security Architecture	Utilize existing 3GPP standard interfaces 3GPP TS 33.401
Security	IP Network Layer Security	Utilize existing 3GPP standard interfaces 3GPP TS 33.210
Security	Session Border Controller - based SIP Interconnection	Utilize existing 3GPP standard TS 29.238 and IETF RFC 5853
Security	IKE with certificates	Utilize existing 3GPP standard interfaces 3GPP TS 33.310
Security	IPSec, Firewall	RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301– Firewall Enhancement Protocol (FEP)
Transmission	Standard connectivity	Industry standard best practice with appropriate security measures and redundancy to meet objectives
Management	Telecommunications Management	Utilize existing 3GPP standard interfaces 3GPP TS 32.101, 3GPP TS 32.102, GSMA IR.88

7.3 StdV-2 PSTN/ISP Interface Roadmap

The Contractor shall comply with the standards in its PSTN/ISP Interface roadmap to support mission-critical communication services that are required in the FOC timeline:

- Mission-critical video and data
- MC-PTT enhancements
- ProSe enhancements
- GCSE enhancements
- Enhanced location services for indoor and outdoor emergency communications

8 Applications Ecosystem Interface (Interface #6)

The applications ecosystem interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

The key interfaces of the application ecosystem in the NPSBN are:

1. The public safety app developers, partners, and their applications
2. The device ecosystem and its applications
3. The Public Safety Entity, their network and the applications

The Contractor shall comply with the interface specification standard and security policies outlined in Section J, Attachment J-10, Cybersecurity, for the applications ecosystem.

8.1 SV-1 Applications Ecosystem Interface (Interface #6)

The following system view diagram depicts the applications ecosystem interface.

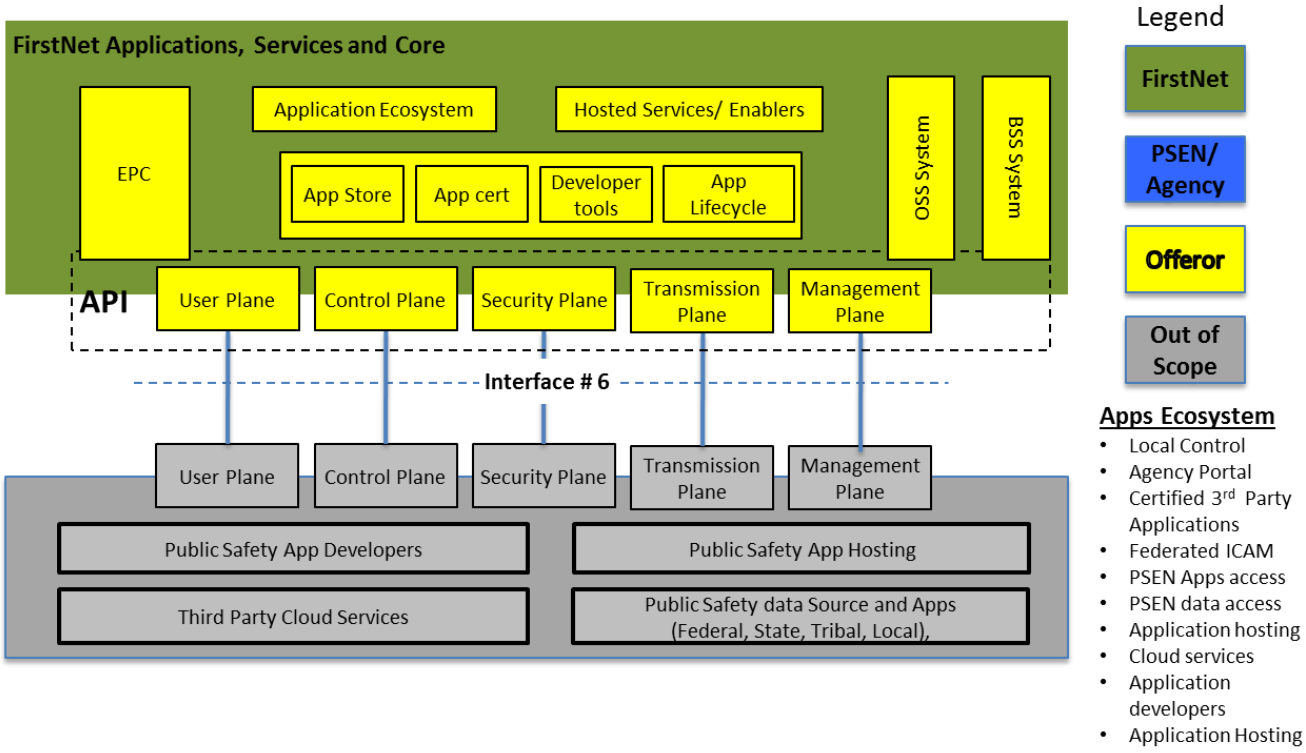


Figure 7 SV-1 Applications Ecosystem

8.2 StdV-1 Applications Ecosystem Interface (Interface #6)

The standards and the source document defined in the tables below for the interface provides minimum guidance to the Contractors.

The Contractor shall comply with the interface specification standard, security policy outlined in Section J, Attachment J-10, Cybersecurity, for the application ecosystem.

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on application interfaces that may not be available at IOC but are expected to be operational at FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 6 StdV-1 Applications Ecosystem Interface Specifications.

Table 6 StdV-1 Applications Ecosystem Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	Federated ICAM Credentials and Credentialing. Authentication and SSO Authorization and ABAC	Utilize industry standard best practices. Some of the minimum Federated ICAM standards and best practice are: GFIPM: Global Federated Identity and Privilege Management NIEF: National Identity Exchange Federation FICAM: Federal Identity, Credential and Access Management SICAM: State Identity, Credential and Access Management. OASIS SAML 2.0 Open ID Connect (http://openid.net/connect/) Kantara Initiative (https://kantarainitiative.org/) NISTIR – 8014 ATIS-1000044.2011 ATIS-1000045.2012 FIPS 201-2 NIST SP 800-157 NIST SP 800-78-4 NIST SP 800-73-4 NIST SP 800-76-2 NIST SP 800-63-2 FIDO: Fast Identity Online NIST SP 800-79-2 NSIT SP 1800-3 (Draft)
User	Third-Party Apps (FirstNet-certified)	Utilize industry standard best practices.
User	Offeror-Provided App (Local Control, PSE home page)	Utilize industry standard best practices.
User	APIs	Utilize industry standard best practices for network, device, OSS, BSS, and cloud services.
User	App Store	Utilize industry standard best practices

Service Area (Plane)	Description	Standard and Source Document
User	App Developer App certification and tools. App Life-cycle	Utilize industry standard best practices. SDK, API, plugins, and development tools available for native, hybrid, web, desktop applications for all of the device types in the device ecosystem. OWASP NIST-SP-163 NIST NVD Static, Dynamic, Interactive analysis test tools for applications and its security (SAST, DAST, IAST) following industry standard best practice and methods Utilize industry standard best practices
User	App Security	Section J, Attachment J-10, Cybersecurity, app security guidelines. Utilize industry standard best practices.
User	ProSe PC1 – App server to UE PC2 – Core to App server	Utilize existing 3GPP standard interfaces or industry best practices. 3GPP TS 23.303 3GPP TS 24.333 3GPP TS 24.334 3GPP TS 36.843 3GPP TS 29.345
User	Locations Services lr RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
Control	ICS and Rx	Utilize existing 3GPP standard interfaces or industry best practices
Security		Utilize existing 3GPP standard interfaces
Security	IPsec, Firewall	Section J, Attachment J-10, Cybersecurity RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301– Firewall Enhancement Protocol (FEP)
Security	Federated ICAM	Refer ICAM user plane standards related to security guidelines and utilize industry standard best practice.
Transmission		Utilize industry standard best practices
Management	Local Control System and component Management Tools	Utilize existing 3GPP standard interfaces or industry best practices Industry standard best practice for data collection

8.3 StdV-2 Applications Ecosystem Interface Roadmap

The applications ecosystem interface at FOC shall be compliant with the then-current 3GPP release standards.

9 Public Safety Enterprise Network Interface (Interface #7)

The PSEN interface will support existing services, features, and applications as specified in 3GPP releases and in accordance with Section J, Attachment J-8, IOC/FOC Target Timeline, for all user, control, security, transmission, and management planes.

The specification defines the interface and relevant standards between a PSEN and FirstNet domains, enabling secure access by first responders to the databases, services, and applications that are hosted by the PSEN, as well as interworking with FirstNet functions, applications, and services.

FirstNet's intent is not to be prescriptive in how the logical interfaces displayed are implemented. FirstNet's intention is to work with the Contractor to solidify key PSEN interface requirements to ensure proper connectivity, services, application, security, and functionality objectives of each PSEN interface are met.

9.1 SV-1 Public Safety Enterprise Network Interface (Interface #7)

The following system view diagram depicts the PSEN interface.

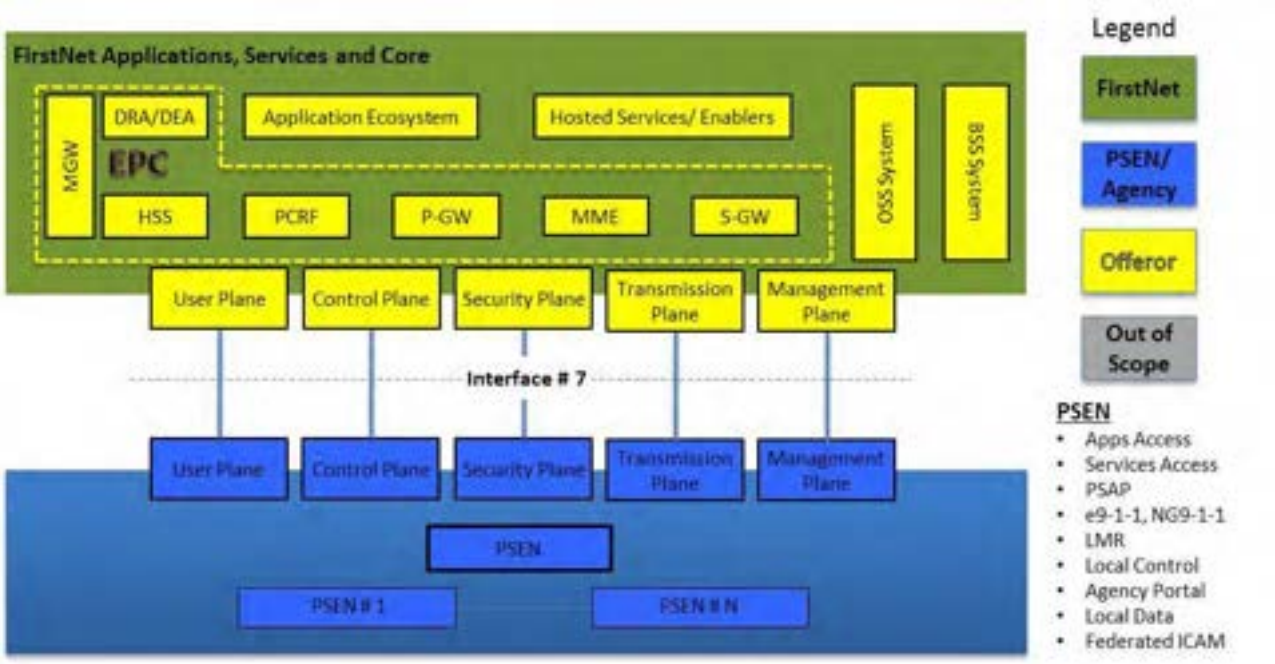


Figure 8 SV-1 PSEN

9.2 StdV-1 Public Safety Enterprise Network Interface (Interface #7)

This section defines system-level interfaces, functionality, and standards, which are expected to be deployed during IOC and available at FOC. The focus is on key PSEN capabilities that will be available at IOC and are expected to be operational through FOC. It also identifies those areas that may impact the interface between the NPSBN and other subsystems as well as critical technology standards affecting future development and maintainability of the NPSBN.

The Contractor shall comply with the mandatory standards interface specification requirements for interoperability with the NPSBN found in Table 7 StdV-1 PSEN Interface Specifications.

Table 7 StdV-1 PSEN Interface Specifications

Service Area (Plane)	Description	Standard and Source Document
User	IMS peering for NG911 Multimedia Services	3GPP TS23.167, Emergency Services IP Network Design for NG9-1-1 Information Document (http://www.nena.org/?page=Standards)
User	Third Party Apps (FirstNet certified)	Utilize industry standard best practices.
User	App Security	Section J, Attachment J-10, Cybersecurity, app security guidelines. Utilize industry standard best practices.
User	Federated ICAM Credentials and Credentialing Authentication and SSO Authorization and ABAC	Utilize industry standard best practices. Some of the minimum Federated ICAM standards and best practice are: GFIPM: Global Federated Identity and Privilege Management NIEF: National Identity Exchange Federation FICAM: Federal Identity, Credential, and Access Management SICAM: State Identity, Credential, and Access Management. OASIS SAML 2.0 Open ID Connect Kantara initiative NISTIR – 8014 ATIS-1000044.2011 ATIS-1000045.2012 FIPS 201-2 NIST SP 800-157 NIST SP 800-78-4 NIST SP 800-73-4 NIST SP 800-76-2 NIST SP 800-63-2 FIDO: Fast Identity Online NIST SP 800-79-2 NSIT SP 1800-3 (Draft)
User	VoLTE	VoLTE IR.92 version 6?
User	MC-PTT	3GPP TS 22.179, TS 23.779
User	GSCE/SC-PTM	3GPP TS 22.179 3GPP TS 22.468 3GPP TS 36.890 SC-PTM TS 36.890

Service Area (Plane)	Description	Standard and Source Document
User	ProSe PC1: Applications to UE PC2: Core to App server	3GPP TS 23.703 3GPP TS 23.713 3GPP TS 23.303 3GPP TS 24.333 3GPP TS 24.334 3GPP TS 36.843 3GPP TS 29.345
User	Locations Services lr RLP	3GPP TS 23.271 OMA-TS-RLP-V1_2-20120529-C
User	Enhanced Messaging	
Control		Utilize existing 3GPP standard interfaces
Control	Ici/Izi	3GPP TS 29.165 [24], GSMA PRD IR.65
Security	IPSec, Firewall	Section J, Attachment J-10, Cybersecurity RFC 4301 (Security Architecture for the Internet Protocol), AH and ESP RFC 4301 – Firewall Enhancement Protocol (FEP) Firewall Policy Implementation (VPN) Utilize existing 3GPP standard interfaces TBD added security standards
Security	ICAM	FIPS140-2, levels 2 and 3 (Suite B)
Security	Authentication of users	SAML2.0 or Open ID Connect tokens Derived PIV-I, NIST SP 800-157
Security	Identification of endpoints, users, and devices	PKI X.509 v3 Radius/ PKI for smartcards, user certificates (such as PIV-I), tokens and biometric systems. Radius-EAP protocol with Active Directory
Transmission	Transmission Point of Presence (POP) for public and private peering and point to point circuits	Utilize existing 3GPP and industry standard interfaces for layers 1, 2 and 3 transmission connectivity such as fiber, copper, microwave and satellite, Ethernet, MPLS, VPLS and appropriate hardening and redundancy mechanisms to separate domains (BGP, OSPF, etc.) as well as isolate and eliminate data storms
Management	Local Control QoS and access policies for provisioning	Utilize existing 3GPP and industry standard interfaces or industry best practices such as Web interface/HTTP(S)
Management	Device Management (includes applications)	Utilize existing industry standard interfaces or industry best practices such as Web interface/ HTTP(S) to multi-tenant OMA-DM v2.0 compliant system
Management	CRM	Utilize existing industry standard interfaces or industry best practices such as Web interface/ HTTP(S)
Management	Monitoring, SLAs	Utilize existing industry standard interfaces or industry best practices such as Web interface/ HTTP(S)

Service Area (Plane)	Description	Standard and Source Document
Management	Accounting	Utilize existing industry standard interfaces or industry best practices such as Web interface/ HTTP(S)
Management	Priority and Quality of Service	Utilize existing 3GPP standard interfaces or industry best practices, TLS
Management	FCAPS, ITIL, NGNMS	Utilize existing 3GPP standard interfaces or industry best practices such as RFC 3411 SNMP v3, FTP, sftp, 3GPP TS 32.102

9.3 StdV-2 Public Safety Enterprise Network Interface Roadmap

The PSEN interface roadmap is the technical standards description of each of the identified additional interfaces required at FOC. The standards described in the table shall meet the current general release version at the time of FOC (standards forecast Release 14 and other standards planned for IOC-4 to FOC time frame).

The following table lists any application and service extensions that may not be available during the IOC time frames. These may include such items as data sharing, computer-aided dispatch (CAD), location, NG9-1-1, and ESINet integration.

Table 8 StdV-2 PSEN Application and Service Extension Interface Specifications

Service Area	Subset	Standard and Source Document
User	CAD application	APCO and IJIS Institute on CAD minimum functional requirements for multi-functional, multi-discipline PSEN https://www.apcointl.org/doc/911-resources/apco-standards/584-11011-2015-multi-functional-multi-discipline-cad/file.html
User	NG9-1-1	Data apps sharing with FirstNet
User	ESINet	Data apps sharing with FirstNet
Security	ESINet	Section J, Attachment J-10, Cybersecurity Future cybersecurity standards
User	Information Sharing Environment (ISE)	DHS-ISE: Information Sharing Environment National Strategy for Information Sharing and Safeguarding (NSISS) https://www.ise.gov

Questions Template

Company Name:	
Point of Contact Name:	
Point of Contact Title:	
Point of Contact Email Address:	
Point of Contact Phone Number:	

Item	Page No.	Document	Section Number	Paragraph Reference/ Sentence	Question
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					

Table of Contents

List of Tables

1 Purpose of the Quality Assurance Surveillance Plan

The Contractor shall provide a Quality Assurance Surveillance Plan (QASP) that defines what the Government and the Contractor must do to ensure the Contractor has performed in accordance with the performance metrics/standards as agreed upon in the contract. Additionally, the QASP is intended to provide a plan to assess the performance of the Contractor in meeting the First Responder Network Authority's (FirstNet) Statement of Objectives (SOO), as defined in Section C. The Contractor is responsible for management and quality control actions required to meet the terms of the contract. The Government reserves the right to perform, with the Contractor, quality assurance (QA) and surveillance in order to verify contract performance standards are achieved and maintained throughout the life of the contract. The Government reserves the right to independently conduct these reviews with full Contractor participation and cooperation.

The proposed QASP should leverage industry best practices, technology enhancements, and professional expertise. The plan should employ standard business practices and processes and minimize risk while improving quality of service.

The QASP is intended to establish procedures pertaining to the assessment/inspection process that may be conducted. The QASP should address the following questions:

- What will be monitored?
- How will monitoring take place?
- Who will conduct the monitoring?
- How will monitoring efforts and results be documented?

Section F, Deliverables and Performance, requests Offerors to include a list of reports and/or other deliverables that will document contractual compliance and Contractor performance. Documented results from the QASP should be formally reported to the Government via deliverables detailed in Section F, Deliverables and Performance, as they are finalized at contract award.

The QASP shall include, at a minimum, a surveillance matrix that clearly states the method(s) of surveillance to be used. The QASP must address how the Contractor will measure, assess, manage, and report on the quality of its performance.

The QASP is a "living document" that will be incorporated into the resulting contract, and the Government may review and revise it on a quarterly basis in coordination with the Contractor. Updates will ensure that the QASP remains a valid, useful, and enforceable document. Copies of the original QASP and revisions will be retained in the contract file.

2 Roles and Responsibilities: Government Personnel

The personnel described below shall oversee and coordinate surveillance activities. For specific appointees for the following roles, see Section G, Contract Administration Data.

2.1 Contracting Officer

The Contracting Officer (CO) shall ensure performance of all contractually required actions, ensure compliance with the contract terms and conditions, and safeguard the interests of the Government in the contractual agreement. The CO shall also ensure that the Contractor receives impartial, fair, and equitable treatment under this contract. The CO is ultimately responsible for the final determination of the adequacy of the Contractor's performance.

2.2 Contracting Officer's Representative

The Contracting Officer's Representative (COR) is responsible for providing continuous technical oversight of the Contractor's performance. The COR will use the QASP to conduct the oversight/surveillance process. The COR shall maintain a QA file that accurately documents the Contractor's actual performance. The purpose is to ensure the Contractor meets the performance metrics/standards contained in the contract. The COR is responsible for reporting any performance issues and/or problems to the CO immediately. The COR is required to provide an annual performance assessment to the CO that may be utilized in documenting past performance. The QASP is a primary tool for analyzing Contractor performance. The COR is not empowered to make any contractual commitments or to authorize any contractual change on FirstNet's behalf. The CO will designate a COR at time of award.

3 Performance Requirements

Performance requirements define desired services and the level of service required under the contract to successfully meet the performance objective. The Government will perform surveillance to determine if the Contractor exceeds, meets, or does not meet these requirements. The Offeror shall provide as part of its proposal a QASP, including but not limited to a QASP surveillance matrix.

The Contractor shall ensure that all aspects of contractual performance are monitored, including but not limited to the following:

- Network performance
- Device usage, operation, and performance
- Application usage, operation, and performance
- Sales and marketing performance and forecasting
- Customer care, including customer satisfaction, issue resolution, activation, etc.
- Business metrics, including financial reports validating sustainability, revenues from spectrum monetization, and user fees
- Interfaces with state-deployed Radio Access Networks and performance therein
- Product planning and roadmap

4 Surveillance Matrix

The Contractor shall organize and document the proposed QASP surveillance matrix in accordance with the format defined in Section J, Attachment J-9, QASP Surveillance Matrix Template. The Contractor's proposed QASP surveillance matrix should include metrics that address each objective described in the SOO and the respective performance standards.

The COR uses the methods contained in Section 4.5, Method of Surveillance, to ensure the Contractor complies with contract performance metrics/standards. The COR is responsible for a wide range of surveillance requirements that effectively measure and assess the Contractor's performance.

The following descriptions detail the sections of the QASP surveillance matrix.

4.1 QASP Identification Number

The QASP Surveillance Matrix (Section J, Attachment J-9) lists each performance metric or standard using a unique identifier.

4.2 Purpose

For each QASP element, the QASP Surveillance Matrix (Section J, Attachment J-9) describes the intended purpose of the QASP element.

4.3 Performance Standard

The QASP Surveillance Matrix (Section J, Attachment J-9) includes brief summary descriptions of the indicators that will be used to monitor each QASP element.

4.4 Acceptable Performance Level

The Government will use Acceptable Performance Levels (APLs) to determine the Contractor's performance. Each QASP element should include an APL in the form of a quantifiable, measurable metric.

4.5 Method of Surveillance

The QASP Surveillance Matrix (Section J, Attachment J-9) includes the method of surveillance for each QASP element. The method of surveillance defines how, when, and what will be monitored and assessed in measuring performance. Acceptable surveillance methods include periodic, 100 percent inspection, inspection of reports, technical inspection, and customer complaint surveillance.

4.5.1 Periodic

Periodic surveillance/inspection is defined as sampling that occurs less than 100 percent of the time or that may be conducted on a statistically random basis. Periodic surveillance can be accomplished weekly, monthly, or quarterly and will be determined by the Government.

4.5.2 100% Inspection

The 100 percent inspection method is designed to evaluate all outputs of a contract requirement. This method requires a total inspection of the Contractor's performance.

4.5.3 Inspection of Reports

All reports shall be reviewed upon receipt by the COR or as otherwise designated. The COR will report any deficiencies in each document.

4.5.4 Technical Inspection

Technical surveillance/inspection will be performed as specified on the project schedule by observing the work being done. For example, the Government reserves the right to observe any applicable testing.

4.5.5 Customer Complaint Surveillance

The customer complaint surveillance is initiated when the COR receives a programmatic or contractual-related complaint from a Public Safety Entity (PSE) regarding Contractor service. The COR will obtain the complaint in writing, document the complaint using the Customer Complaint Record (CCR) form, available in Section 6.2, Customer Complaint Record, and conduct an investigation to determine its validity. If the complaint is deemed valid, the COR will take action as outlined in Section 5.2, Remedies for Non-Conformance.

4.6 Measures and Metrics

The QASP Surveillance Matrix includes detailed descriptions of how each QASP element will be measured.

4.7 Performance Target

Each QASP element will be measured against the performance ratings described in Section 5.1, Performance Rating Definitions. The QASP Surveillance Matrix lists the appropriate performance rating based on the measure described in Section 4.6, Measures and Metrics.

4.8 Calculation and Formulas

The QASP Surveillance Matrix includes detailed descriptions of how the measures described in Section 4.6, Measures and Metrics are calculated.

4.9 Statement of Objectives Reference

For each QASP element, the QASP Surveillance Matrix lists the corresponding objectives (as defined in Section C, SOO) that the metric/standard addresses.

5 Performance Rating

Based upon the performance metrics/standards and APLs defined in the Offeror's proposed QASP, the COR will measure the Contractor's performance using the following performance rating methodology.

5.1 Performance Rating Definitions

In evaluating the Contractor's performance, the performance ratings outlined in Table 1 Performance Rating Definitions will be used.

Table 1 Performance Rating Definitions

Performance Rating	Criteria
Blue – Excellent/ Outstanding	Performance exceeds performance metrics/standards and benefits FirstNet. The QASP element being assessed was accomplished with no problems and Contractor actions were highly effective.
Green – Good	Performance meets the metrics/standards. The performance contains minor problems for which corrective actions taken by the Contractor were satisfactory.
Yellow – Marginal	Performance does not meet some metrics/standards. The performance reflects a serious problem for which the Contractor has not yet identified corrective actions. The Contractor's proposed actions appear marginally effective or were not fully implemented.
Red – Unsatisfactory	Performance does not meet most metrics/standards and corrective action is not likely to be completed in a timely manner. The performance contains serious problem(s) for which the Contractor's corrective actions appear or were ineffective.

5.2 Remedies for Non-Conformance

If inspections indicate unacceptable performance and/or deficiencies, the COR will notify the Contractor's program manager and task manager of the deficiencies for correction. This will normally be in writing unless circumstances necessitate verbal communication. Regardless, the COR will document the discussion and place it in the COR contract file. The Contractor shall be given an agreed-upon time frame (depending on the discrepancy identified) after notification to correct the unacceptable performance or deficiency. If the performance or deficiency is not corrected within the required time frame, the COR will notify the CO for action, which may include remedies. If the Contractor disagrees with the noted discrepancy and an agreement cannot be reached, the CO will be notified to assist with a final determination.

5.3 Disincentive Payments

Upon the Contractor's failure to meet performance metrics associated with the adoption and use of the Nationwide Public Safety Broadband Network (NPSBN) by public safety users, FirstNet will assess the Contractor with a disincentive payment.

5.3.1 Public Safety Device Connection Targets

The Offeror shall propose public safety device connection targets (connection targets), which represent the Offeror's anticipated number of public safety device connections (device connections) for law enforcement, fire, emergency medical services, and other public safety users by each of the 56 states and territories over the life of the contract, as detailed in Section L, Instructions, Conditions, and Notices to Offerors or Respondents. For the purposes of this disincentive mechanism, FirstNet defines a device connection as a device on a post-paid contract with an eligible NPSBN user that has been generating billable revenue for three consecutive months. Each device connection will be assigned to the state or territory based on the registered billing address of that device connection. The connection targets will serve as the basis for the disincentive mechanism structure further described below.

5.3.2 Disincentive Payment Calculation and Timing

The Contractor is subject to disincentive payments beginning at the start of the first Government fiscal year following Final Operational Capability (FOC) (i.e., the FOC performance year). These payments may continue over the remaining period of performance based on achievement measured against the Contractor's proposed connection targets. The date of initial device activation on the NPSBN shall determine in which FOC performance year a device shall be considered for disincentive payment calculations. FirstNet reserves the right to an audit, at FirstNet's sole discretion, to ensure device connections on the network are (1) devices that match the aforementioned definition, (2) in use by a defined user group, (3) and accurate in quantity. In addition to complying with all applicable federal and state data retention requirements—including applicable Federal Communications Commission rules and policies—regarding the NPSBN, for purposes of ensuring FirstNet's audit rights, the Contractor is required to retain all applicable data required to perform the audit for a period of four (4) years.

5.3.3 Adjustment for Government Fiscal Year after FOC

The Contractor's proposed connection targets in the Public Safety Device Connections Template (Section J, Attachment J-24) will be adjusted using a weighted average methodology to align with the Government fiscal year, for purposes of this disincentive mechanism. The weighted average connection targets are calculated by taking the sum of the proposed connection targets in the Public Safety Device Connections Template for each year and multiplying it by the number of calendar days of the Government fiscal year covered by those forecasts, and then dividing the resulting sum by 365 days. For example, if the actual task order date for a state or territory is June 1, 2017, and the proposed FOC date is May 31, 2022, the start of the first Government fiscal year following FOC is Oct 1, 2022, then connections targets for the first Government fiscal year following FOC are calculated as:

Connections targets for the Government fiscal year 2023 = [(connections targets for period ending May 31, 2023 x 243 days/365 days) + (connections targets for period ending May 31, 2024 x 122 days/365 days)]. The resulting sum will be rounded up to the nearest whole number.

This will be repeated on an annual basis for each state and territory for purposes of calculating the total disincentive payments for the life of the IDIQ contract.

5.3.4 User Groups

PSEs are defined in the Middle Class Tax Relief and Job Creation Act of 2012 (the Act); however, for the purpose of this disincentive mechanism, FirstNet further delineates PSEs into two user groups: a primary user group and extended primary user group. FirstNet prefers device connections from the primary user group, which consists of law enforcement, fire, and emergency medical services users. The Contractor is also encouraged to drive customer adoption and use of the NPSBN through the extended primary user group, which consists of all other public safety users, as defined in the Act. The Contractor will be subject to disincentive payments upon failure to achieve 100 percent of the proposed connection targets for either user group.

5.3.5 Maximum Disincentive Payments

The maximum value of disincentive payments, subject to the Contractor's performance against its proposed connection targets, is spread across each FOC performance year as shown in Table 2 Total Maximum Disincentive Payments by State/Territory Across FOC Performance Years. The total maximum disincentive payments per state and territory is calculated by dividing the total annual maximum

disincentive payment into two categories—population and state and territory—each of which contains 50 percent of the total annual maximum disincentive payment amount. The population category is distributed to each of the 56 states and territories based on the state or territory's population as a percentage of the total population for all 56 states and territories. The state and territory category is equally distributed among all 56 states and territories with each state and territory receiving the same weight. The aggregate value from the population and state and territory categories comprises the annual maximum disincentive payment for the state or territory. For FOC performance years beyond Year 20, an annual inflation factor of 1.9% will be applied on annual basis.

Table 2 Total Maximum Disincentive Payments by State/Territory Across FOC Performance Years

FOC Performance Year	1	2	3	4	5	6	7	8	9	10
Annual disincentive payment	$ 124,704,388	$ 127,073,771	$ 129,488,173	$ 131,948,448	$ 134,455,469	$ 137,010,123	$ 139,613,315	$ 142,265,968	$ 144,969,021	$ 147,723,433
Alabama	$ 2,066,062	$ 2,105,318	$ 2,145,319	$ 2,186,080	$ 2,227,615	$ 2,269,940	$ 2,313,069	$ 2,357,017	$ 2,401,800	$ 2,447,435
Alaska	$ 1,254,985	$ 1,278,830	$ 1,303,128	$ 1,327,887	$ 1,353,117	$ 1,378,826	$ 1,405,024	$ 1,431,720	$ 1,458,922	$ 1,486,642
American Samoa	$ 1,124,497	$ 1,145,863	$ 1,167,634	$ 1,189,819	$ 1,212,426	$ 1,235,462	$ 1,258,936	$ 1,282,855	$ 1,307,230	$ 1,332,067
Arizona	$ 2,387,400	$ 2,432,760	$ 2,478,983	$ 2,526,084	$ 2,574,079	$ 2,622,987	$ 2,672,823	$ 2,723,607	$ 2,775,356	$ 2,828,087
Arkansas	$ 1,694,592	$ 1,726,789	$ 1,759,598	$ 1,793,031	$ 1,827,098	$ 1,861,813	$ 1,897,188	$ 1,933,234	$ 1,969,966	$ 2,007,395
California	$ 8,538,371	$ 8,700,601	$ 8,865,912	$ 9,034,364	$ 9,206,017	$ 9,380,932	$ 9,559,169	$ 9,740,793	$ 9,925,869	$ 10,114,460
Colorado	$ 2,115,781	$ 2,155,981	$ 2,196,945	$ 2,238,687	$ 2,281,222	$ 2,324,565	$ 2,368,732	$ 2,413,738	$ 2,459,599	$ 2,506,331
Connecticut	$ 1,825,771	$ 1,860,461	$ 1,895,810	$ 1,931,830	$ 1,968,535	$ 2,005,937	$ 2,044,050	$ 2,082,887	$ 2,122,462	$ 2,162,788
Delaware	$ 1,292,396	$ 1,316,951	$ 1,341,973	$ 1,367,471	$ 1,393,453	$ 1,419,928	$ 1,446,907	$ 1,474,398	$ 1,502,412	$ 1,530,958
District of Columbia	$ 1,233,359	$ 1,256,793	$ 1,280,672	$ 1,305,005	$ 1,329,800	$ 1,355,066	$ 1,380,812	$ 1,407,048	$ 1,433,782	$ 1,461,023
Florida	$ 4,860,647	$ 4,952,999	$ 5,047,106	$ 5,143,002	$ 5,240,719	$ 5,340,292	$ 5,441,758	$ 5,545,151	$ 5,650,509	$ 5,757,869
Georgia	$ 3,044,240	$ 3,102,081	$ 3,161,020	$ 3,221,080	$ 3,282,280	$ 3,344,643	$ 3,408,192	$ 3,472,947	$ 3,538,933	$ 3,606,173
Guam	$ 1,145,193	$ 1,166,952	$ 1,189,124	$ 1,211,717	$ 1,234,740	$ 1,258,200	$ 1,282,106	$ 1,306,466	$ 1,331,288	$ 1,356,583
Hawaii	$ 1,384,548	$ 1,410,855	$ 1,437,661	$ 1,464,976	$ 1,492,811	$ 1,521,174	$ 1,550,077	$ 1,579,528	$ 1,609,539	$ 1,640,121
Idaho	$ 1,425,861	$ 1,452,952	$ 1,480,558	$ 1,508,689	$ 1,537,354	$ 1,566,563	$ 1,596,328	$ 1,626,658	$ 1,657,565	$ 1,689,059
Illinois	$ 3,670,655	$ 3,740,397	$ 3,811,465	$ 3,883,883	$ 3,957,676	$ 4,032,872	$ 4,109,497	$ 4,187,577	$ 4,267,141	$ 4,348,217
Indiana	$ 2,405,693	$ 2,451,401	$ 2,497,978	$ 2,545,439	$ 2,593,803	$ 2,643,085	$ 2,693,304	$ 2,744,476	$ 2,796,622	$ 2,849,757
Iowa	$ 1,720,589	$ 1,753,280	$ 1,786,593	$ 1,820,538	$ 1,855,128	$ 1,890,375	$ 1,926,293	$ 1,962,892	$ 2,000,187	$ 2,038,191
Kansas	$ 1,682,076	$ 1,714,035	$ 1,746,602	$ 1,779,787	$ 1,813,603	$ 1,848,062	$ 1,883,175	$ 1,918,955	$ 1,955,415	$ 1,992,568
Kentucky	$ 1,978,294	$ 2,015,882	$ 2,054,184	$ 2,093,213	$ 2,132,984	$ 2,173,511	$ 2,214,807	$ 2,256,889	$ 2,299,770	$ 2,343,465
Louisiana	$ 2,016,961	$ 2,055,283	$ 2,094,333	$ 2,134,126	$ 2,174,674	$ 2,215,993	$ 2,258,097	$ 2,301,000	$ 2,344,719	$ 2,389,269
Maine	$ 1,378,182	$ 1,404,368	$ 1,431,051	$ 1,458,241	$ 1,485,947	$ 1,514,180	$ 1,542,950	$ 1,572,266	$ 1,602,139	$ 1,632,580
Maryland	$ 2,264,136	$ 2,307,155	$ 2,350,990	$ 2,395,659	$ 2,441,177	$ 2,487,559	$ 2,534,823	$ 2,582,984	$ 2,632,061	$ 2,682,070
Massachusetts	$ 2,418,414	$ 2,464,364	$ 2,511,187	$ 2,558,900	$ 2,607,519	$ 2,657,062	$ 2,707,546	$ 2,758,989	$ 2,811,410	$ 2,864,827
Michigan	$ 3,083,301	$ 3,141,884	$ 3,201,580	$ 3,262,410	$ 3,324,396	$ 3,387,559	$ 3,451,923	$ 3,517,509	$ 3,584,342	$ 3,652,445
Minnesota	$ 2,170,536	$ 2,211,777	$ 2,253,800	$ 2,296,623	$ 2,340,258	$ 2,384,723	$ 2,430,033	$ 2,476,204	$ 2,523,252	$ 2,571,193
Mississippi	$ 1,704,832	$ 1,737,224	$ 1,770,231	$ 1,803,866	$ 1,838,139	$ 1,873,064	$ 1,908,652	$ 1,944,917	$ 1,981,870	$ 2,019,525
Missouri	$ 2,307,062	$ 2,350,896	$ 2,395,563	$ 2,441,078	$ 2,487,459	$ 2,534,721	$ 2,582,880	$ 2,631,955	$ 2,681,962	$ 2,732,919
Montana	$ 1,310,628	$ 1,335,530	$ 1,360,905	$ 1,386,763	$ 1,413,111	$ 1,439,960	$ 1,467,320	$ 1,495,199	$ 1,523,607	$ 1,552,556
Nebraska	$ 1,477,433	$ 1,505,504	$ 1,534,109	$ 1,563,257	$ 1,592,959	$ 1,623,225	$ 1,654,066	$ 1,685,493	$ 1,717,518	$ 1,750,151
Nevada	$ 1,651,668	$ 1,683,050	$ 1,715,028	$ 1,747,613	$ 1,780,818	$ 1,814,654	$ 1,849,132	$ 1,884,266	$ 1,920,067	$ 1,956,548
New Hampshire	$ 1,375,812	$ 1,401,953	$ 1,428,590	$ 1,455,733	$ 1,483,392	$ 1,511,577	$ 1,540,297	$ 1,569,562	$ 1,599,384	$ 1,629,772
New Jersey	$ 2,865,710	$ 2,920,158	$ 2,975,641	$ 3,032,179	$ 3,089,790	$ 3,148,496	$ 3,208,317	$ 3,269,275	$ 3,331,392	$ 3,394,688
New Mexico	$ 1,523,839	$ 1,552,792	$ 1,582,295	$ 1,612,358	$ 1,642,993	$ 1,674,210	$ 1,706,020	$ 1,738,435	$ 1,771,465	$ 1,805,123
New York	$ 4,975,605	$ 5,070,142	$ 5,166,475	$ 5,264,638	$ 5,364,666	$ 5,466,594	$ 5,570,460	$ 5,676,298	$ 5,784,148	$ 5,894,047
North Carolina	$ 3,013,912	$ 3,071,176	$ 3,129,528	$ 3,188,989	$ 3,249,580	$ 3,311,322	$ 3,374,237	$ 3,438,348	$ 3,503,676	$ 3,570,246
North Dakota	$ 1,247,484	$ 1,271,186	$ 1,295,338	$ 1,319,950	$ 1,345,029	$ 1,370,584	$ 1,396,625	$ 1,423,161	$ 1,450,201	$ 1,477,755
Northern Mariana Islands	$ 1,124,161	$ 1,145,520	$ 1,167,285	$ 1,189,464	$ 1,212,063	$ 1,235,093	$ 1,258,559	$ 1,282,472	$ 1,306,839	$ 1,331,669
Ohio	$ 3,412,727	$ 3,477,569	$ 3,543,643	$ 3,610,972	$ 3,679,581	$ 3,749,493	$ 3,820,733	$ 3,893,327	$ 3,967,300	$ 4,042,679
Oklahoma	$ 1,861,099	$ 1,896,460	$ 1,932,493	$ 1,969,210	$ 2,006,625	$ 2,044,751	$ 2,083,601	$ 2,123,190	$ 2,163,530	$ 2,204,637
Oregon	$ 1,876,988	$ 1,912,651	$ 1,948,991	$ 1,986,022	$ 2,023,757	$ 2,062,208	$ 2,101,390	$ 2,141,316	$ 2,182,001	$ 2,223,460
Pennsylvania	$ 3,645,093	$ 3,714,350	$ 3,784,923	$ 3,856,836	$ 3,930,116	$ 4,004,788	$ 4,080,879	$ 4,158,416	$ 4,237,426	$ 4,317,937
Puerto Rico	$ 1,856,004	$ 1,891,268	$ 1,927,203	$ 1,963,819	$ 2,001,132	$ 2,039,153	$ 2,077,897	$ 2,117,377	$ 2,157,608	$ 2,198,602
Rhode Island	$ 1,323,215	$ 1,348,356	$ 1,373,975	$ 1,400,080	$ 1,426,682	$ 1,453,789	$ 1,481,411	$ 1,509,558	$ 1,538,239	$ 1,567,466
South Carolina	$ 2,035,295	$ 2,073,966	$ 2,113,371	$ 2,153,525	$ 2,194,442	$ 2,236,137	$ 2,278,623	$ 2,321,917	$ 2,366,033	$ 2,410,988
South Dakota	$ 1,275,703	$ 1,299,941	$ 1,324,640	$ 1,349,808	$ 1,375,455	$ 1,401,588	$ 1,428,219	$ 1,455,355	$ 1,483,007	$ 1,511,184
Tennessee	$ 2,378,249	$ 2,423,436	$ 2,469,481	$ 2,516,401	$ 2,564,213	$ 2,612,933	$ 2,662,579	$ 2,713,168	$ 2,764,718	$ 2,817,248
Texas	$ 6,125,095	$ 6,241,472	$ 6,360,060	$ 6,480,901	$ 6,604,038	$ 6,729,515	$ 6,857,375	$ 6,987,666	$ 7,120,431	$ 7,255,719
Utah	$ 1,664,291	$ 1,695,913	$ 1,728,135	$ 1,760,970	$ 1,794,428	$ 1,828,522	$ 1,863,264	$ 1,898,666	$ 1,934,741	$ 1,971,501
Vermont	$ 1,238,146	$ 1,261,671	$ 1,285,643	$ 1,310,070	$ 1,334,961	$ 1,360,325	$ 1,386,172	$ 1,412,509	$ 1,439,346	$ 1,466,694
Virgin Islands	$ 1,134,639	$ 1,156,197	$ 1,178,165	$ 1,200,550	$ 1,223,361	$ 1,246,605	$ 1,270,290	$ 1,294,426	$ 1,319,020	$ 1,344,081
Virginia	$ 2,708,085	$ 2,759,538	$ 2,811,969	$ 2,865,397	$ 2,919,839	$ 2,975,316	$ 3,031,847	$ 3,089,453	$ 3,148,152	$ 3,207,967
Washington	$ 2,453,674	$ 2,500,293	$ 2,547,799	$ 2,596,207	$ 2,645,535	$ 2,695,800	$ 2,747,021	$ 2,799,214	$ 2,852,399	$ 2,906,595
West Virginia	$ 1,482,745	$ 1,510,917	$ 1,539,625	$ 1,568,877	$ 1,598,686	$ 1,629,061	$ 1,660,013	$ 1,691,554	$ 1,723,693	$ 1,756,443
Wisconsin	$ 2,246,883	$ 2,289,574	$ 2,333,076	$ 2,377,404	$ 2,422,575	$ 2,468,604	$ 2,515,507	$ 2,563,302	$ 2,612,004	$ 2,661,632
Wyoming	$ 1,225,766	$ 1,249,056	$ 1,272,788	$ 1,296,971	$ 1,321,613	$ 1,346,724	$ 1,372,312	$ 1,398,385	$ 1,424,955	$ 1,452,029
Total	$ 124,704,388	$ 127,073,771	$ 129,488,173	$ 131,948,448	$ 134,455,469	$ 137,010,123	$ 139,613,315	$ 142,265,968	$ 144,969,021	$ 147,723,433

FOC Performance Year	11	12	13	14	15	16	17	18	19	20
Annual disincentive payment	$ 150,530,178	$ 153,390,251	$ 156,304,666	$ 159,274,455	$ 162,300,670	$ 165,384,382	$ 168,526,686	$ 171,728,693	$ 174,991,538	$ 178,316,377
Alabama	$ 2,493,936	$ 2,541,321	$ 2,589,606	$ 2,638,808	$ 2,688,946	$ 2,740,036	$ 2,792,096	$ 2,845,146	$ 2,899,204	$ 2,954,289
Alaska	$ 1,514,888	$ 1,543,671	$ 1,573,001	$ 1,602,888	$ 1,633,342	$ 1,664,376	$ 1,695,999	$ 1,728,223	$ 1,761,059	$ 1,794,519
American Samoa	$ 1,357,376	$ 1,383,166	$ 1,409,447	$ 1,436,226	$ 1,463,514	$ 1,491,321	$ 1,519,656	$ 1,548,530	$ 1,577,952	$ 1,607,933
Arizona	$ 2,881,821	$ 2,936,576	$ 2,992,370	$ 3,049,226	$ 3,107,161	$ 3,166,197	$ 3,226,355	$ 3,287,655	$ 3,350,121	$ 3,413,773
Arkansas	$ 2,045,536	$ 2,084,401	$ 2,124,004	$ 2,164,360	$ 2,205,483	$ 2,247,387	$ 2,290,088	$ 2,333,600	$ 2,377,938	$ 2,423,119
California	$ 10,306,635	$ 10,502,461	$ 10,702,008	$ 10,905,346	$ 11,112,547	$ 11,323,686	$ 11,538,836	$ 11,758,074	$ 11,981,477	$ 12,209,125
Colorado	$ 2,553,951	$ 2,602,476	$ 2,651,923	$ 2,702,310	$ 2,753,654	$ 2,805,973	$ 2,859,287	$ 2,913,613	$ 2,968,972	$ 3,025,382
Connecticut	$ 2,203,881	$ 2,245,755	$ 2,288,424	$ 2,331,904	$ 2,376,211	$ 2,421,359	$ 2,467,364	$ 2,514,244	$ 2,562,015	$ 2,610,693
Delaware	$ 1,560,046	$ 1,589,687	$ 1,619,891	$ 1,650,669	$ 1,682,031	$ 1,713,990	$ 1,746,556	$ 1,779,740	$ 1,813,555	$ 1,848,013
District of Columbia	$ 1,488,783	$ 1,517,070	$ 1,545,894	$ 1,575,266	$ 1,605,196	$ 1,635,695	$ 1,666,773	$ 1,698,442	$ 1,730,712	$ 1,763,596
Florida	$ 5,867,268	$ 5,978,746	$ 6,092,342	$ 6,208,097	$ 6,326,051	$ 6,446,246	$ 6,568,724	$ 6,693,530	$ 6,820,707	$ 6,950,301
Georgia	$ 3,674,690	$ 3,744,509	$ 3,815,655	$ 3,888,152	$ 3,962,027	$ 4,037,306	$ 4,114,015	$ 4,192,181	$ 4,271,832	$ 4,352,997
Guam	$ 1,382,358	$ 1,408,623	$ 1,435,387	$ 1,462,659	$ 1,490,450	$ 1,518,768	$ 1,547,625	$ 1,577,030	$ 1,606,993	$ 1,637,526
Hawaii	$ 1,671,283	$ 1,703,037	$ 1,735,395	$ 1,768,367	$ 1,801,966	$ 1,836,204	$ 1,871,092	$ 1,906,642	$ 1,942,869	$ 1,979,783
Idaho	$ 1,721,151	$ 1,753,853	$ 1,787,176	$ 1,821,132	$ 1,855,734	$ 1,890,993	$ 1,926,922	$ 1,963,533	$ 2,000,840	$ 2,038,856
Illinois	$ 4,430,833	$ 4,515,019	$ 4,600,804	$ 4,688,220	$ 4,777,296	$ 4,868,064	$ 4,960,558	$ 5,054,808	$ 5,150,850	$ 5,248,716
Indiana	$ 2,903,903	$ 2,959,077	$ 3,015,299	$ 3,072,590	$ 3,130,969	$ 3,190,458	$ 3,251,076	$ 3,312,847	$ 3,375,791	$ 3,439,931
Iowa	$ 2,076,916	$ 2,116,378	$ 2,156,589	$ 2,197,564	$ 2,239,318	$ 2,281,865	$ 2,325,220	$ 2,369,399	$ 2,414,418	$ 2,460,292
Kansas	$ 2,030,427	$ 2,069,005	$ 2,108,316	$ 2,148,374	$ 2,189,193	$ 2,230,788	$ 2,273,173	$ 2,316,363	$ 2,360,374	$ 2,405,221
Kentucky	$ 2,387,991	$ 2,433,363	$ 2,479,597	$ 2,526,709	$ 2,574,717	$ 2,623,636	$ 2,673,485	$ 2,724,282	$ 2,776,043	$ 2,828,788
Louisiana	$ 2,434,665	$ 2,480,924	$ 2,528,061	$ 2,576,095	$ 2,625,040	$ 2,674,916	$ 2,725,740	$ 2,777,529	$ 2,830,302	$ 2,884,077
Maine	$ 1,663,599	$ 1,695,207	$ 1,727,416	$ 1,760,237	$ 1,793,681	$ 1,827,761	$ 1,862,489	$ 1,897,876	$ 1,933,936	$ 1,970,680
Maryland	$ 2,733,030	$ 2,784,957	$ 2,837,871	$ 2,891,791	$ 2,946,735	$ 3,002,723	$ 3,059,775	$ 3,117,910	$ 3,177,151	$ 3,237,517
Massachusetts	$ 2,919,258	$ 2,974,724	$ 3,031,244	$ 3,088,838	$ 3,147,526	$ 3,207,329	$ 3,268,268	$ 3,330,365	$ 3,393,642	$ 3,458,121
Michigan	$ 3,721,841	$ 3,792,556	$ 3,864,615	$ 3,938,042	$ 4,012,865	$ 4,089,110	$ 4,166,803	$ 4,245,972	$ 4,326,645	$ 4,408,852
Minnesota	$ 2,620,046	$ 2,669,827	$ 2,720,554	$ 2,772,244	$ 2,824,917	$ 2,878,590	$ 2,933,283	$ 2,989,016	$ 3,045,807	$ 3,103,677
Mississippi	$ 2,057,896	$ 2,096,996	$ 2,136,839	$ 2,177,439	$ 2,218,811	$ 2,260,968	$ 2,303,926	$ 2,347,701	$ 2,392,307	$ 2,437,761
Missouri	$ 2,784,845	$ 2,837,757	$ 2,891,674	$ 2,946,616	$ 3,002,602	$ 3,059,651	$ 3,117,785	$ 3,177,023	$ 3,237,386	$ 3,298,896
Montana	$ 1,582,054	$ 1,612,113	$ 1,642,744	$ 1,673,956	$ 1,705,761	$ 1,738,170	$ 1,771,196	$ 1,804,848	$ 1,839,140	$ 1,874,084
Nebraska	$ 1,783,403	$ 1,817,288	$ 1,851,817	$ 1,887,001	$ 1,922,854	$ 1,959,388	$ 1,996,617	$ 2,034,552	$ 2,073,209	$ 2,112,600
Nevada	$ 1,993,722	$ 2,031,603	$ 2,070,203	$ 2,109,537	$ 2,149,619	$ 2,190,461	$ 2,232,080	$ 2,274,490	$ 2,317,705	$ 2,361,741
New Hampshire	$ 1,660,738	$ 1,692,292	$ 1,724,445	$ 1,757,210	$ 1,790,597	$ 1,824,618	$ 1,859,286	$ 1,894,612	$ 1,930,610	$ 1,967,292
New Jersey	$ 3,459,187	$ 3,524,912	$ 3,591,885	$ 3,660,131	$ 3,729,673	$ 3,800,537	$ 3,872,747	$ 3,946,330	$ 4,021,310	$ 4,097,715
New Mexico	$ 1,839,420	$ 1,874,369	$ 1,909,982	$ 1,946,272	$ 1,983,251	$ 2,020,933	$ 2,059,330	$ 2,098,458	$ 2,138,328	$ 2,178,956
New York	$ 6,006,034	$ 6,120,148	$ 6,236,431	$ 6,354,923	$ 6,475,667	$ 6,598,705	$ 6,724,080	$ 6,851,837	$ 6,982,022	$ 7,114,681
North Carolina	$ 3,638,081	$ 3,707,204	$ 3,777,641	$ 3,849,417	$ 3,922,555	$ 3,997,084	$ 4,073,029	$ 4,150,416	$ 4,229,274	$ 4,309,630
North Dakota	$ 1,505,832	$ 1,534,443	$ 1,563,598	$ 1,593,306	$ 1,623,579	$ 1,654,427	$ 1,685,861	$ 1,717,892	$ 1,750,532	$ 1,783,792
Northern Mariana Islands	$ 1,356,971	$ 1,382,753	$ 1,409,025	$ 1,435,797	$ 1,463,077	$ 1,490,876	$ 1,519,202	$ 1,548,067	$ 1,577,480	$ 1,607,452
Ohio	$ 4,119,490	$ 4,197,760	$ 4,277,517	$ 4,358,790	$ 4,441,607	$ 4,525,998	$ 4,611,992	$ 4,699,620	$ 4,788,912	$ 4,879,902
Oklahoma	$ 2,246,525	$ 2,289,209	$ 2,332,704	$ 2,377,026	$ 2,422,189	$ 2,468,211	$ 2,515,107	$ 2,562,894	$ 2,611,589	$ 2,661,209
Oregon	$ 2,265,705	$ 2,308,754	$ 2,352,620	$ 2,397,320	$ 2,442,869	$ 2,489,283	$ 2,536,580	$ 2,584,775	$ 2,633,885	$ 2,683,929
Pennsylvania	$ 4,399,978	$ 4,483,577	$ 4,568,765	$ 4,655,572	$ 4,744,028	$ 4,834,164	$ 4,926,013	$ 5,019,608	$ 5,114,980	$ 5,212,165
Puerto Rico	$ 2,240,376	$ 2,282,943	$ 2,326,319	$ 2,370,519	$ 2,415,559	$ 2,461,454	$ 2,508,222	$ 2,555,878	$ 2,604,440	$ 2,653,924
Rhode Island	$ 1,597,248	$ 1,627,595	$ 1,658,520	$ 1,690,032	$ 1,722,142	$ 1,754,863	$ 1,788,205	$ 1,822,181	$ 1,856,803	$ 1,892,082
South Carolina	$ 2,456,797	$ 2,503,476	$ 2,551,042	$ 2,599,512	$ 2,648,902	$ 2,699,232	$ 2,750,517	$ 2,802,777	$ 2,856,030	$ 2,910,294
South Dakota	$ 1,539,896	$ 1,569,154	$ 1,598,968	$ 1,629,349	$ 1,660,306	$ 1,691,852	$ 1,723,997	$ 1,756,753	$ 1,790,131	$ 1,824,144
Tennessee	$ 2,870,775	$ 2,925,320	$ 2,980,901	$ 3,037,538	$ 3,095,252	$ 3,154,061	$ 3,213,988	$ 3,275,054	$ 3,337,280	$ 3,400,689
Texas	$ 7,393,578	$ 7,534,056	$ 7,677,203	$ 7,823,070	$ 7,971,708	$ 8,123,171	$ 8,277,511	$ 8,434,784	$ 8,595,045	$ 8,758,350
Utah	$ 2,008,959	$ 2,047,129	$ 2,086,025	$ 2,125,659	$ 2,166,047	$ 2,207,202	$ 2,249,139	$ 2,291,872	$ 2,335,418	$ 2,379,791
Vermont	$ 1,494,561	$ 1,522,958	$ 1,551,894	$ 1,581,380	$ 1,611,426	$ 1,642,043	$ 1,673,242	$ 1,705,034	$ 1,737,429	$ 1,770,441
Virgin Islands	$ 1,369,619	$ 1,395,641	$ 1,422,158	$ 1,449,179	$ 1,476,714	$ 1,504,771	$ 1,533,362	$ 1,562,496	$ 1,592,183	$ 1,622,435
Virginia	$ 3,268,918	$ 3,331,028	$ 3,394,317	$ 3,458,809	$ 3,524,527	$ 3,591,493	$ 3,659,731	$ 3,729,266	$ 3,800,122	$ 3,872,324
Washington	$ 2,961,820	$ 3,018,094	$ 3,075,438	$ 3,133,872	$ 3,193,415	$ 3,254,090	$ 3,315,918	$ 3,378,920	$ 3,443,120	$ 3,508,539
West Virginia	$ 1,789,816	$ 1,823,822	$ 1,858,475	$ 1,893,786	$ 1,929,768	$ 1,966,433	$ 2,003,796	$ 2,041,868	$ 2,080,663	$ 2,120,196
Wisconsin	$ 2,712,203	$ 2,763,735	$ 2,816,246	$ 2,869,755	$ 2,924,280	$ 2,979,842	$ 3,036,459	$ 3,094,151	$ 3,152,940	$ 3,212,846
Wyoming	$ 1,479,617	$ 1,507,730	$ 1,536,377	$ 1,565,568	$ 1,595,314	$ 1,625,625	$ 1,656,512	$ 1,687,986	$ 1,720,057	$ 1,752,738
Total	$ 150,530,178	$ 153,390,251	$ 156,304,666	$ 159,274,455	$ 162,300,670	$ 165,384,382	$ 168,526,686	$ 171,728,693	$ 174,991,538	$ 178,316,377

5.3.5.1 Disincentive Payment Calculation

The Contractor's connection targets at the state/territory level will be used to evaluate actual performance and determine the level of disincentive payment required to FirstNet, when performance falls below targets in any given year. The disincentive payment will be calculated to reflect FirstNet's preference of public safety connections from the primary user group over the extended primary user group (see description in Section 5.3.4, User Groups). Specifically, the annual maximum disincentive payment for each state or territory will be split and applied based on the achievement of primary user group connection targets (65 percent of the annual maximum disincentive payments) and the achievement of extended user group connection targets (35 percent of the annual maximum disincentive payments). The Contractor is liable for disincentive payments upon failure to achieve 100 percent of either target, in a given year. Percentage points will be rounded to the nearest full percentage. For clarity, percentages will be rounded up for any percentage above 0.5 percent.

FirstNet will use a progressive scale to calculate the disincentive payment. To encourage focus and effort on high levels of public safety adoption, FirstNet will use a progressive scale to calculate the disincentive payment. For each percentage point below 100 percent achievement of the proposed connection target in each state/territory and year, FirstNet will apply increasingly higher disincentive payment. With this structure, the Contractor incurs a larger disincentive payment per percentage point as target achievement approaches the 70 percent floor. Refer to Table 3 Progressive Scale for Disincentive Payments for further details on FirstNet's scale to measure disincentive payments. For performance achieved at or above 100 percent of the proposed connection targets for either user group, no monetary mechanisms will be applied.

Table 3 Progressive Scale for Disincentive Payments

User Group Connection Target Achieved	Disincentive Payment	Performance Remediation Action
100%	0%	No action
99%	1%	
98%	2%	
97%	3%	
96%	5%	
95%	6%	
94%	8%	
93%	9%	
92%	11%	
91%	13%	
90%	15%	
89%	17%	The Contractor develops and implements a corrective action plan to increase public safety adoption to 100%
88%	19%	
87%	21%	
86%	24%	
85%	27%	
84%	30%	
83%	33%	
82%	36%	
81%	40%	
80%	44%	

User Group Connection Target Achieved	Disincentive Payment	Performance Remediation Action
79%	48%	FirstNet may exercise its rights (in accordance with laws and regulations) and request the Contractor to provide discounted pricing to meet targets
78%	52%	
77%	57%	
76%	62%	
75%	67%	
74%	73%	
73%	79%	
72%	86%	
71%	93%	
70%	100%	
<70%	100%	FirstNet may exercise its rights (in accordance with laws and regulations) to either own or contract out functions responsible for driving public safety adoption at the Contractor's cost

5.3.5.2 Reporting and Payment

The Contractor must provide a quarterly device connections (see Section F, Deliverables and Performance) report to FirstNet throughout the government fiscal year for the period of performance. The report, at minimum, should consist of the following: gross activations, gross deactivations, net connections, total connections, quarterly churn, and reasons for churn (e.g., voluntary churn, involuntary churn), as well as be able to break down the aforementioned data by primary user group and extended primary user group by device type and monthly data usage at a state/territory level. FirstNet will charge the applicable disincentive payment to the Contractor based on the total net device connections at the end of each Government fiscal year relative to the Offeror's proposed connection targets (as detailed in Section J, Attachment J-24, Public Safety Device Connections Template), the disincentives in Table 2 Total Maximum Disincentive Payments by State/Territory Across FOC Performance Years, and the calculations in Table 3 Progressive Scale for Disincentive Payments. Any disincentive payments should be made by the Contractor to FirstNet no later than January 31 of the following Government fiscal year.

5.3.5.3 Performance Remediation

Public safety adoption and use of the NPSBN are primary FirstNet programmatic objectives. It is important that the Contractor maintain and grow public safety adoption throughout the life of the contract. Should the Contractor's performance fail to meet or maintain connection targets, appropriate actions may be exercised at FirstNet's discretion, in addition to the disincentive payment program described above.

Table 4 Performance Remediation Triggers identifies additional performance remediation triggers should the Contractor's total missed connection targets (primary user group and extended primary user group) surpass 10 percent of the forecasted connection target in any state/territory and year. Remediation is triggered if either of the following is met:

- Total missed connections targets exceed 10 percent in three or more quarters over a period of six consecutive quarters for either the primary user group or extended primary user group
- Total missed connections targets exceed 10 percent in two consecutive quarters for either the primary user group or extended primary user group

Table 4 Performance Remediation Triggers

Trigger	Cause	Performance Remediation Action
1	Contractor misses 10% to 20% of its connection targets in three of six consecutive quarters or two consecutive quarters	Contractor develops and implements a corrective action plan to increase public safety adoption to 100%
2	Contractor misses 20% to 30% of its connection targets in three of six consecutive quarters or two consecutive quarters	FirstNet may exercise its rights (in accordance with laws and regulations) and request the Contractor to provide discounted pricing to meet targets
3	Contractor misses 30% or more of its connection targets in three of six consecutive quarters or two consecutive quarters	FirstNet may exercise its rights (in accordance with laws and regulations) to either own or contract out functions responsible for driving public safety adoption at the Contractor's cost

Performance remediation will cease or reduce as the Contractor achieves two consecutive quarters of performance at a trigger level lower than its current level of performance in line with the performance shortfall described in Table 4 Performance Remediation Triggers.

5.4 Performance Assessment Report

Performance Assessment Reports (PARs), available in Section 6.3, Performance Assessment Report, will be used to report all minor discrepancies and will be generated by the COR and sent to the Contractor for corrective action with a copy sent to the CO. The Contractor will be given ten (10) business days to correct PARs unless another date is mutually agreed upon. If three minor discrepancies are found during one month of performance, the Contractor shall submit a corrective action plan to the COR with a copy sent to the CO.

5.5 Corrective Action Report

When there is a deficiency and the COR determines that formal written communication is required, the COR will prepare a Corrective Action Report (CAR) and present it to the Contractor's program manager and task manager. A CAR template is available in Section 6.1, Corrective Action Report. The CAR will identify the performance problem along with the proposed resolution and the scheduled date for correction. The Contractor shall be required to acknowledge receipt of the CAR in writing. The CAR will specify if the Contractor is required to prepare a corrective action plan to document how the Contractor shall correct the unacceptable performance and avoid a recurrence. The CAR will also state how long after receipt the Contractor has to present this corrective action plan to the COR. The Government will review the Contractor's corrective action plan to determine acceptability. The Contractor shall provide a weekly status of the corrective action until all performance problems have been satisfactorily resolved. Any CAR will become a part of the supporting documentation; the Government will use any corrective

action documentation as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

6 Forms

Examples of forms for the PAR, CAR, and CCR can be found in this section. The specific format or content of these forms may be modified at a later date to better capture information required to achieve the objectives described above.

6.1 Corrective Action Report

CORRECTIVE ACTION REPORT (If more space is needed, use reverse and identify by number)		
1. CONTRACTOR	2. CONTRACT NUMBER	3. TYPE OF SERVICES
4. FUNCTIONAL AREA	5. SUSPENSE DATE	6. CONTROL NUMBER
7. DEFICIENCY ☐ MAJOR ☐ MINOR FINDING: FINDING IMPACT: Please respond with a written corrective action plan that details the corrective action of the cited deficiency, the cause of the deficiency, and actions taken to prevent recurrence by the suspense date cited in Block 5. If no date was entered in Block 5, the Contractor is not required to provide a response.		
8. QUALITY ASSURANCE PERSONNEL (COR)		
TYPED NAME AND GRADE	SIGNATURE AND DATE	
9. ISSUING AUTHORITY		
TYPED NAME AND GRADE	SIGNATURE AND DATE	
10. COR RESPONSE TO CONTRACTOR CORRECTIVE ACTION AND ACTION TAKEN TO PREVENT RECURRENCE		
11. COR DETERMINATION ☐ ACCEPTED ☐ REJECTED	12. CLOSE DATE	

6.2 Customer Complaint Record

CUSTOMER COMPLAINT RECORD			DATE/TIME OF COMPLAINT
SOURCE OF COMPLAINT			
ORGANIZATION	LOCATION	INDIVIDUAL	PHONE NUMBER
NATURE OF COMPLAINT			
CONTRACT REFERENCE			
VALIDATION			
DATE/TIME CONTRACTOR INFORMED OF COMPLAINT			
ACTION TAKEN BY CONTRACTOR			
RECEIVED/VALIDATED BY			

6.3 Performance Assessment Report

PERFORMANCE ASSESSMENT REPORT (If more space is needed, use reverse and identify by number)			
1. CONTRACT/TASK ORDER NUMBER	2. CONTRACTOR	3. TYPE OF SERVICES	
4. QUALITY ASSURANCE PERSONNEL (COR) SIGNATURE AND DATE		5. COR PHONE	6. SUSPENSE DATE
I. PERFORMANCE			
7. ☐ DEFICIENCY (CHECK ALL BOXES THAT APPLY) ☐ NEW ☐ REPEAT ☐ NO DEFICIENCY NOTED		8. SERVICES SUMMARY OR (STATEMENT OF WORK) PARAGRAPH ITEM REVIEWED	
9. BRIEF DESCRIPTION OF DEFICIENCY (IF DEFICIENCY BOX WAS CHECKED)		10. DETAILED PERFORMANCE ASSESSMENT	
II. CONTRACTOR VALIDATION			
11. CONTRACTOR REPRESENTATIVE ☐ CONCUR ☐ NON-CONCUR		12. CORRECTIVE ACTION ESTIMATED COMPLETION DATE	
13. CONTRACTOR REPRESENTATIVE CORRECTIVE ACTION AND PREVENTION OF RECURRENCE OR REASON FOR NON-CONCURRENCE OF COR-CITED DEFICIENCY			
III. ACTION CORRECTED			
14. ☐ CONCUR ☐ NON-CONCUR COR SIGNATURE AND DATE			
15. COR REMARKS (REQUIRED)			
6. CONTRACTOR REPRESENTATIVE REMARKS			

7 Signatures

Contracting Officer

_____ Date: _____

Contracting Officer's Representative

_____ Date: _____

Alternate Contracting Officer's Representative

_____ Date: _____

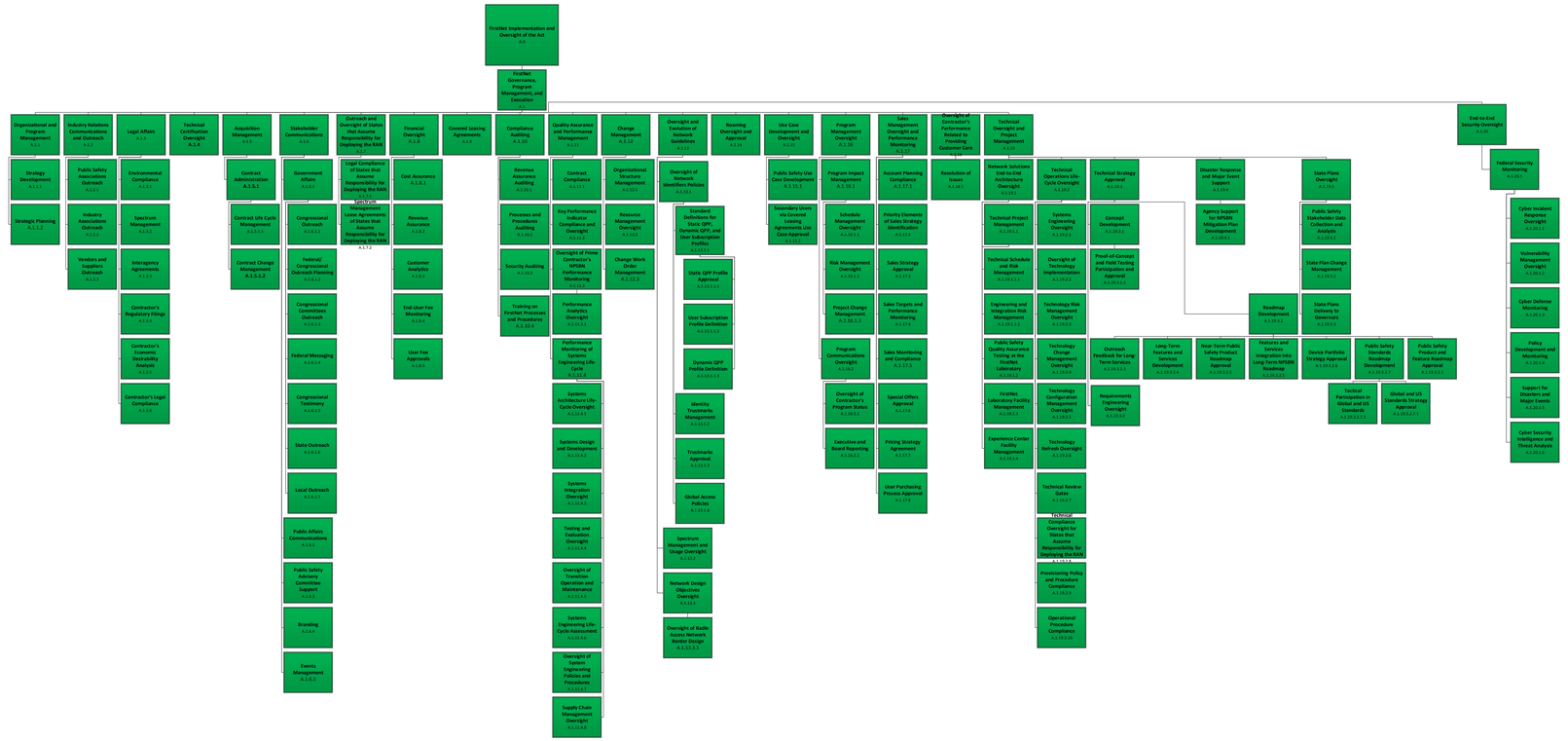

FirstNet Implementation and Oversight of the Act
A.0
FirstNet Governance, Program Management, and Execution
A.1
Organizational and Program Management
A.1.1
Strategy Development
A.1.1.1
Strategic Planning
A.1.1.2
Industry Relation Communications and Outreach
A.1.2
Public Safety Associations Outreach
A.1.2.1
Industry Associations Outreach
A.1.2.2
Vendors and Suppliers Outreach
A.1.2.3
Legal Affairs
A.1.3
Environmental Compliance
A.1.3.1
Spectrum Management
A.1.3.2
Interagency Agreements
A.1.3.3
Contractor's Regulatory Filings
A.1.3.4
Contractor's Economic Desirability Analysis
A.1.3.5
Contractor's Legal Compliance
A.1.3.6
Technical Certification Oversight
A.1.4
Acquisition Management
A.1.5
Contract Administration
A.1.5.1
Contract Life Cycle Management
A.1.5.1.1
Contract Change Management
A.1.5.1.2
Stakeholder Communications
A.1.6
Government Affairs
A.1.6.1
Congressional Outreach
A.1.6.1.1
Federal/ Congressional Outreach Planning
A.1.6.1.2
Congressional Committees Outreach
A.1.6.1.3
Federal Messaging
A.1.6.1.4
Congressional Testimony
A.1.6.1.5
State Outreach
A.1.6.1.6
Local Outreach
A.1.6.1.7
Public Affairs Communications
A.1.6.2
Public Safety Advisory Committee Support
A.1.6.3
Branding
A.1.6.4
Events Management
A.1.6.5
Outreach and Oversight of States that Assume Responsibility for Deploying the RAN
A.1.7
Legal Compliance of States that Assume Responsibility for Deploying the RAN
A.1.7.1
Spectrum Management Lease Agreements of States that Assume Responsibility for Deploying the RAN
A.1.7.2
Financial Oversight
A.1.8
Cost Assurance
A.1.8.1
Revenue Assurance
A.1.8.2
Customer Analytics
A.1.8.3
End-User Fee Monitoring
A.1.8.4
User Fee Approvals
A.1.8.5
Covered Leasing Agreements
A.1.9
Compliance Auditing
A.1.10
Revenue Assurance Auditing
A.1.10.1
Processes and Procedures Auditing
A.1.10.2
Security Auditing
A.1.10.3
Training on FirstNet Processes and Procedures
A.1.10.4
Quality Assurance and Performance Management
A.1.11
Contract Compliance
A.1.11.1
Key Performance Indicator Compliance and Oversight
A.1.11.2
Oversight of Prime Contractor's NPSBN Performance Monitoring
A.1.11.3
Performance Analytics Oversight
A.1.11.3.1
Performance Monitoring of Systems Engineering Life-Cycle
A.1.11.3.2
Systems Architecture Life-Cycle Oversight
A.1.11.3.3
Systems Design and Development
A.1.11.3.4
Systems Integration Oversight
A.1.11.3.5
Testing and Evaluation Oversight
A.1.11.3.6
Oversight of Transition Operation and Maintenance
A.1.11.3.7
Systems Engineering Life-Cycle Assessment
A.1.11.3.8
Oversight of System Engineering Policies and Procedures
A.1.11.3.9
Supply Chain Management Oversight
A.1.11.3.10
Change Management
A.1.12
Organizational Structure Management
A.1.12.1
Resource Management Oversight
A.1.12.2
Change Work Order Management
A.1.12.3
Oversight and Evolution of Network Guidelines
A.1.13
Oversight of Network Identifiers Policies
A.1.13.1
Standard Definitions for Static QPP, Dynamic QPP, and User Subscription Profiles
A.1.13.1.1
Static QPP Profile Approval
A.1.13.1.1.1
User Subscription Profile Definition
A.1.13.1.1.2
Dynamic QPP Profile Definition
A.1.13.1.1.3
Identity Trustmarks Management
A.1.13.1.2
Trustmarks Approval
A.1.13.1.3
Global Access Policies
A.1.13.1.4
Spectrum Management and Usage Oversight
A.1.13.2
Network Design Objectives Oversight
A.1.13.3
Oversight of Radio Access Network Border Design
A.1.13.3.1
Roaming Oversight and Approval
A.1.14
Use Case Development and Oversight
A.1.15
Public Safety Use Case Development
A.1.15.1
Secondary-Users via Covered Leasing Agreements Use Case Approval
A.1.15.2
Program Management Oversight
A.1.16
Program Impact Management
A.1.16.1
Schedule Management Oversight
A.1.16.1.1
Risk Management Oversight
A.1.16.1.2
Project Change Management
A.1.16.1.3
Program Communications Oversight
A.1.16.2
Oversight of Contractor's Program Status
A.1.16.2.1
Executive and Board Reporting
A.1.16.2.2
Sales Management Oversight and Performance Monitoring
A.1.17
Account Planning Compliance
A.1.17.1
Priority Elements of Sales Strategy Identification
A.1.17.1.1
Sales Strategy Approval
A.1.17.2
Sales Targets and Performance Monitoring
A.1.17.4
Sales Monitoring and Compliance
A.1.17.5
Special Offers Approval
A.1.17.6
Pricing Strategy Agreement
A.1.17.7
User Purchasing Process Approval
A.1.17.8
Oversight of Contractor's Performance Related to Providing Customer Care
A.1.18
Resolution of Issues
A.1.18.1
Technical Oversight and Project Management
A.1.19
Network Solutions End-to-End Architecture Oversight
A.1.19.1
Technical Project Management
A.1.19.1.1
Technical Schedule and Risk Management
A.1.19.1.1.1
Engineering and Integration Risk Management
A.1.19.1.1.2
Public Safety Quality Assurance Testing at the FirstNet Laboratory
A.1.19.1.2
FirstNet Laboratory Facility Management
A.1.19.1.3
Experience Center Facility Management
A.1.19.1.4
Technical Operations Life-Cycle Oversight
A.1.19.2
Systems Engineering Oversight
A.1.19.2.1
Oversight of Technology Implementation
A.1.19.2.1
Technology Risk Management Oversight
A.1.19.2.2
Technology Change Management Oversight
A.1.19.2.4
Technology Configuration Management Oversight
A.1.19.2.5
Technology Refresh Oversight
A.1.19.2.6
Technical Review Gates
A.1.19.2.7
Technical Compliance Oversight for States that Assume Responsibility for Deploying the RAN
A.1.19.2.8
Provisioning Policy and Procedure Compliance
A.1.19.2.9
Operational Procedure Compliance
A.1.19.2.10
Technical Strategy Approval
A.1.19.3
Concept Development
A.1.19.3.1
Proof-of-Concept and Field Testing Participation and Approval
A.1.19.3.1.1
Outreach Feedback for Long-Term Services
A.1.19.3.1.3
Requirements Engineering Oversight
A.1.19.3.1.5
Long-Term Features and Services Development
A.1.19.3.1.4
Near-Term Public Safety Product Roadmap Approval
A.1.19.3.1.2
Features and Services Integration Into Long-Term NPSBN Roadmap
A.1.19.3.1.6
Disaster Response and Major Event Support
A.1.19.4
Agency Support Requirements Mission Plan Development
A.1.19.4.1
Roadmap Development
A.1.19.3.2
State Plans Oversight
A.1.19.5
Public Safety Stakeholder Data Collection and Analysis
A.1.19.5.1
State Plan Change Management
A.1.19.5.2
State Plans Delivery to Governors
A.1.19.5.3
Device Portfolio Strategy Approval
A.1.19.3.2.6
Tactical Participation in Global and US Standards
A.1.19.3.2.7.2
Public Safety Standards Roadmap Development
A.1.19.3.2.7
Global and US Standards Strategy Approval
A.1.19.3.2.7.1
Public Safety Product and Feature Roadmap Approval
A.1.19.3.2.1
End-to-End Security Oversight
A.1.20
Federal Security Monitoring
A.1.20.1
Cyber Incident Response Oversight
A.1.20.1.1
Vulnerability Management Oversight
A.1.20.1.2
Cyber Defense Monitoring
A.1.20.1.3
Policy Development and Monitoring
A.1.20.1.4
Support for Disasters and Major Events
A.1.20.1.5
Cyber Security Intelligence and Threat Analysis
A.1.20.1.6

Table of Contents

1 Operational Architecture

1.1 Inherently Governmental Functions

The First Responder Network Authority (FirstNet) is responsible for ensuring the overall success of the Nationwide Public Safety Broadband Network (NPSBN). In order to do so, FirstNet has developed an Operational Architecture describing high-level functions that FirstNet believes should be executed for the NPSBN to succeed. The Operational Architecture captures the potential scope of FirstNet's overall responsibilities with regard to the NPSBN post award.

Section J, Attachment J-7, Operational Architecture, presents only the inherently governmental functions from the Operational Architecture. As such, these functions would be conducted by FirstNet. An inherently governmental function is defined as any function related to the public interest that mandates performance by government employees. An inherently governmental function includes activities that require either the exercise of discretion in applying government authority or the making of value judgments in making decisions for the Government. Governmental functions normally fall into two categories: the act of governing (i.e., the discretionary exercise of government authority) and monetary transactions and entitlements.

An inherently governmental function involves, among other things, the interpretation and execution of the laws of the United States. Inherently governmental functions do not normally include gathering information for or providing advice, opinions, recommendations, or ideas to government officials. They also do not include functions that are primarily ministerial and internal in nature, such as building security, mail operations, operation of cafeterias, housekeeping, facilities operations and maintenance, warehouse operations, motor vehicle fleet management operations, or other routine electrical or mechanical services.

1.2 Operational Architecture View

The Operational Architecture view in Section J, Attachment J-7, Operational Architecture Visio, provides only the hierarchy of functions that FirstNet may execute in order to ensure the success of the NPSBN. These functions do not represent the entirety of functions that will comprise the NPSBN, only those that FirstNet believes it may execute over the course of the NPSBN contract lifecycle. Additional functions may be identified and executed based on proposed solutions to the objectives identified in Section C, Statement of Objectives. FirstNet's final Operational Architecture is dependent upon the nature and scope of the final award resulting from this Request for Proposal. Offerors should note that these functions do not depict any set of prescriptive requirements and are strictly conceptual in nature.

1.3 Operational Architecture – FirstNet Functions

A.0 FirstNet Implementation and Oversight of the Act

Implements and oversees the Middle Class Tax Relief and Job Creation Act of 2012 (the Act) that created FirstNet as an independent authority within the National Telecommunications and Information Administration (NTIA) to provide first responders with the first nationwide, high-speed, broadband network dedicated to public safety.

A.1 FirstNet Governance, Program Management, and Execution

Establishes FirstNet strategy and organizational processes, procedures, and policies, including program management of Contractor's activities.

A.1.1 Organizational and Program Management

Manages strategy implementation and program execution.

A.1.1.1 Strategy Development

Sets FirstNet's strategic direction, including the facilitation of strategy execution, assessment of program progress, and adherence to strategic milestones.

A.1.1.2 Strategic Planning

Conducts FirstNet strategic planning.

A.1.2 Industry Relations Communications and Outreach

Manages communications and outreach to industries associated with FirstNet, including suppliers, and communicates changing technologies and market demands internally.

A.1.2.1 Public Safety Associations Outreach

Manages communications and outreach to public safety associations.

A.1.2.2 Industry Associations Outreach

Manages communications and outreach to industry associations.

A.1.2.3 Vendors and Suppliers Outreach

Manages communications and outreach to vendors and suppliers to ensure FirstNet-required features and functionalities are represented in roadmaps and rollout schedules.

A.1.3 Legal Affairs

Ensures compliance with the Act and any other applicable laws.

A.1.3.1 Environmental Compliance

Ensures compliance with environmental laws and regulations, including the National Environmental Policy Act.

A.1.3.2 Spectrum Management

Supports FirstNet spectrum management, interference mitigation, and clearing activities, including Federal Communications Commission (FCC) licensing, FCC and NTIA reporting requirements, 3rd Generation Partnership Project (3GPP) standards body interface support, and interface with all other domestic and international standards bodies impacting FirstNet's spectrum position.

A.1.3.3 Interagency Agreements

Develops interagency agreements and monitors compliance with them.

A.1.3.4 Contractor's Regulatory Filings

Reviews and approves Contractor-submitted regulatory filings needed to roll out the NPSBN.

A.1.3.5 Contractor's Economic Desirability Analysis

Reviews and approves the Contractor's economic desirability analysis, which informs the rollout of the NPSBN.

A.1.3.6 Contractor's Legal Compliance

Monitors the Contractor's compliance with all rules, regulations, and laws impacting the rollout of the NPSBN.

A.1.4 Technical Certification Oversight

Oversees the certification and compliance process applicable to the NPSBN.

A.1.5 Acquisition Management

Responsible for managing the acquisition process and for identifying new acquisition opportunities to enhance public safety NPSBN services.

A.1.5.1 Contract Administration

Administers all contracts, including packaging and preparation for release, signatures, and additions/addendums.

A.1.5.1.1 Contract Life-Cycle Management

Manages the life-cycle of all contracts, including renewals, change of scope, and conversions to new contracts.

A.1.5.1.2 Contract Change Management

Manages all contract changes, including redlines, agreements, addendums, and version control through finalization.

A.1.6 Stakeholder Communications

Responsible for communications, outreach, and engagement with FirstNet's stakeholders, including sharing relevant information to assist in understanding the evolving needs of public safety.

A.1.6.1 Government Affairs

Manages outreach and communications with local, state, and federal officials regarding FirstNet.

A.1.6.1.1 Congressional Outreach

Manages outreach and communications with members of Congress, congressional committees, and staff.

A.1.6.1.2 Federal/Congressional Outreach Planning

Develops and implements a federal outreach plan, including congressional outreach.

A.1.6.1.3 Congressional Committees Outreach

Manages outreach and communications with the relevant congressional committee members and staff.

A.1.6.1.4 Federal Messaging

Develops and coordinates messages and communications across the federal government.

A.1.6.1.5 Congressional Testimony

Develops and presents testimony at congressional hearings.

A.1.6.1.6 State Outreach

Manages outreach and communications with state executive and legislative staff.

A.1.6.1.7 Local Outreach

Manages outreach and communications with city and county officials, including county governments, city mayors, town councils, and other local government entities.

A.1.6.2 Public Affairs Communications

Represents FirstNet's interests with local, state, and federal government constituents through proactive outreach and communication, including issuing alerts regarding network problems and failures if and when they occur.

A.1.6.3 Public Safety Advisory Committee Support

Manages meeting planning and administrative services for the Public Safety Advisory Committee, its subcommittees, and associated working groups.

A.1.6.4 Branding

Reviews and approves the brand strategy encompassing network services, evolving applications, and unfolding technologies, including communications methods and materials.

A.1.6.5 Events Management

Coordinates state, tribal, federal, and association conferences, meetings, and events, including in-person events, webinars, and telephone and video conferencing.

A.1.7 Outreach and Oversight of States that Assume Responsibility for Deploying the Radio Access Network

Manages outreach and communications with states and territories that assume responsibility for deploying their own Radio Access Network (RAN) to ensure alignment with evolving network and operational compliance requirements and to solicit inputs on evolving public safety needs.

A.1.7.1 Legal Compliance for States that Assume Responsibility for Deploying the RAN

Monitors efforts by states and territories that assume responsibility for deploying their own RAN, ensuring compliance with all rules, regulations, and laws applicable to FirstNet.

A.1.7.2 Spectrum Management Lease Agreements with States that Assume Responsibility for Deploying the RAN

Supports Spectrum Management Lease Agreements negotiations and agreements with states or territories that assume responsibility for deploying their own RAN and monitors compliance with them.

A.1.8 Financial Oversight

Responsible for financial management of the organization, which incorporates periodic reviews of the Contractor's income and financial statements and includes setting financial plans, monitoring and evaluating the implementation of these plans, and revising them as needed.

A.1.8.1 Cost Assurance

Provides analyses of current and future project costs to ascertain the overall sustainability of the network.

A.1.8.2 Revenue Assurance

Establishes and implements a revenue assurance function for auditing and monitoring receivables, collections, and bad debt from all revenue sources.

A.1.8.3 Customer Analytics

Analyzes customer behavior using market segmentation and predictive analyses, among other methods, to inform key business decisions.

A.1.8.4 End-User Fee Monitoring

Monitors recurring end-user fees regarding their impact to achievement of public safety device connection targets.

A.1.8.5 User Fee Approvals

Seeks NTIA's approval for NPSBN network user fees, network capacity lease fees, and network equipment and infrastructure lease fees.

A.1.9 Covered Leasing Agreements

Responsible for creating the framework for the secondary use of Band 14, negotiating Covered Leasing Agreements with the Contractor and other stakeholders, and monitoring the agreements.

A.1.10 Compliance Auditing

Supports financial, management, and programmatic auditing functions to ensure compliance with all contractual terms and conditions.

A.1.10.1 Revenue Assurance Auditing

Audits and monitors the Contractor's receivables, collections, and bad debt to ensure compliance with all contractual terms and conditions.

A.1.10.2 Processes and Procedures Auditing

Audits the Contractor's and third-party contractor's services and operations processes and procedures to ensure compliance with all contractual terms and conditions.

A.1.10.3 Security Auditing

Audits all security processes and procedures, including support of third-party contractors retained or working on behalf of FirstNet to ensure compliance with all contractual terms and conditions.

A.1.10.4 Training on FirstNet Processes and Procedures

Trains the Contractor on FirstNet processes and procedures.

A.1.11 Quality Assurance and Performance Management

Oversees auditing of the Contractor's Quality Assurance and Surveillance Plan (QASP) to compliance with all contractual terms and conditions. As the QASP evolves over time, the function owner will provide input for metrics and acceptance criteria needed to meet the NPSBN stated objectives.

A.1.11.1 Contract Compliance

Develops, adjusts, and oversees NPSBN contracts to ensure compliance with all contractual terms and conditions by the Contractor and states and territories that assume responsibility for deploying their RAN.

A.1.11.2 Key Performance Indicator Compliance and Oversight

Defines, adjusts, and audits NPSBN Key Performance Indicators, providing oversight to compliance with all contractual terms and conditions.

A.1.11.3 Oversight of Contractor's NPSBN Performance Monitoring

Monitors the overall performance of the NPSBN. Oversees the timely and appropriate resolution of identified performance issues by the Contractor and states and territories that assume responsibility for deploying their RAN.

A.1.11.3.1 Performance Analytics Oversight

Oversees analytics of the NPSBN to identify issues and trends. Works with the Contractor and program management on mitigation.

A.1.11.4 Performance Monitoring of Systems Engineering Life-Cycle

Conducts performance monitoring and oversight of the Contractor's systems engineering life-cycle processes and outcomes for the NPSBN.

A.1.11.4.1 Systems Architecture Life-Cycle Oversight

Oversees the Contractor's system architecture life-cycle processes and outcomes for the NPSBN.

A.1.11.4.2 Systems Design and Development

Oversees the Contractor's performance of the systems design and development for the NPSBN within the service development life-cycle.

A.1.11.4.3 Systems Integration Oversight

Oversees NPSBN systems integration within the integration activity life-cycle.

A.1.11.4.4 Testing and Evaluation Oversight

Oversees the Contractor's testing and evaluation of the NPSBN.

A.1.11.4.5 Oversight of Transition to Operations and Maintenance

Overseesthe Contractor's transition to operations and continuing maintenance of the NPSBN.

A.1.11.4.6 Systems Engineering Life-Cycle Assessment

Oversees and assesses the Contractor's systems engineering life-cycle processes for the NPSBN.

A.1.11.4.7 Oversight of Systems Engineering Policies and Procedures

Oversees systems engineering policies and procedures within the NPSBN to enforce compliance of the engineering life-cycle and evolution of the NPSBN.

A.1.11.4.8 Supply Chain Management Oversight

Oversees all supply chain issues relating to systems engineering life-cycle activities.

A.1.12 Change Management

Reviews, negotiates, and approves Contractor-proposed changes related to technical, financial, or organizational aspects of the NPSBN.

A.1.12.1 Organizational Structure Management

Manages the overall organizational structure to execute the NPSBN in the most efficient manner. Conducts discussions and negotiations with Contractor for required organizational changes in support of change management.

A.1.12.2 Resource Management Oversight

Conducts discussions and negotiations with the Contractor for resource requirement changes in support of change management.

A.1.12.3 Change Work Order Management

Conducts discussions and negotiations with the Contractor for work order changes in support of the expedient execution of the program.

A.1.13 Oversight and Evolution of Network Guidelines

Defines a framework for the high-level network strategy and designs guidelines to ensure optimum network performance for public safety and a ubiquitous experience for FirstNet stakeholders, including the Contractor, states and territories that assume responsibility for deploying their RAN, and FirstNet.

A.1.13.1 Oversight of Network Identifiers Policies

Creates the framework and policies for network identifiers to be used by FirstNet, the Contractor and states and territories that assume responsibility for deploying their RAN to ensure nationwide public safety interoperability and interworking.

A.1.13.1.1 Standard Definitions for Static QPP, Dynamic QPP, and User Subscription Profiles

Develops the user policy for the Quality of Service, Priority, and Preemption (QPP) framework specifically for static (non-emergency), dynamic (emergency), and user subscription profiles (i.e., voice, data, and push-to-talk).

A.1.13.1.1.1 Static QPP Profile Approval

Approves static QPP profiles for appropriate NPSBN services.

A.1.13.1.1.2 User Subscription Profile Definition

Defines all user subscription profiles for NPSBN services such as voice, data, and push-to-talk.

A.1.13.1.1.3 Dynamic QPP Profile Definition

Develops the dynamic QPP profile framework specifically for dynamic, emergency situations.

A.1.13.1.2 Identity Trustmarks Management

Identifies trustmarks, including specific identity-related functionalities, which should be supported as part of the FirstNet federated Identity, Credential, and Access Management (ICAM). Identifies specific trustmarks that are recommended to be supported across agencies in order to more easily achieve

secure access and interoperability (i.e., federated ICAM). Oversees security for the trustmarks to ensure adequate standards are being applied.

A.1.13.1.3 Trustmarks Approval

Creates, updates, and manages vetting of trustmarks that are recommended to be included in the FirstNet federated ICAM.

A.1.13.1.4 Global Access Policies

Defines and provides support of global access policies for the establishment of global identity management.

A.1.13.2 Spectrum Management and Usage Oversight

Creates and monitors the Band 14 spectrum management framework with respect to FirstNet, the Contractor, and states and territories that assume responsibility for deploying their RAN. Monitors and reports Band 14 incumbent transmission transition schedules (to leave/evacuate Band 14 spectrum) and temporary licensees utilizing Band 14.

A.1.13.3 Network Design Objectives Oversight

Defines a framework for network design guidelines to ensure optimum network performance for public safety and a ubiquitous network experience for FirstNet stakeholders, including the Contractor, states and territories that assume responsibility for deploying their RAN, and FirstNet.

A.1.13.3.1 Oversight of Radio Access Network Border Design

Ensures optimal network design and integration of FirstNet cell sites at the border with states and territories that assume responsibility for deploying their RAN and other service providers, thus providing optimum network performance for public safety and a ubiquitous network experience for FirstNet stakeholders, including the Contractor, states and territories that assume responsibility for deploying their RAN, and FirstNet.

A.1.14 Roaming Oversight and Approval

Identifies and develops roaming requirements with the Contractor. Oversees the timely implementation of roaming agreements.

A.1.15 Use Case Development and Oversight

Defines possible use cases for the NPSBN, driving requirements for product management and network design guidelines.

A.1.15.1 Public Safety Use Case Development

Defines public safety use cases, which may drive requirements and design guidelines.

A.1.15.2 Secondary Users via Covered Leasing Agreements Use Case Approval

Defines secondary user use cases via Covered Leasing Agreements associated with the NPSBN, which may drive requirements and design guidelines.

A.1.16 Program Management Oversight

Directly manages the FirstNet program staff, both federal and Contractor, utilizing known and accepted program management methods (e.g., Project Management Institute, Agile) to manage the outcomes and performance of the program.

A.1.16.1 Program Impact Management

Assesses program impacts and identifies potential strategies or solutions to mitigate or reduce impacts to the program.

A.1.16.1.1 Schedule Management Oversight

Oversees the Contractor's management of all program schedules, including the definition, approval, and assignment of the program schedule. Schedule management includes tasks, priorities, assignments, dependencies, resources, timing and slippage, and critical path assessments.

A.1.16.1.2 Risk Management Oversight

Assesses program risks and identifies potential strategies or solutions to mitigate or reduce risks to the program.

A.1.16.1.3 Project Change Management

Manages all changes to the program. Management includes the definition, approval, and assignment of the change within the program. Changes range from technical to procedural and may include timing and resource requirements.

A.1.16.2 Program Communications Oversight

Manages the communications of all program statuses. Communications includes the reporting of milestone completions, resource utilization, and slippage and timing of deliverables to keep the project or program on track, including issue and roadblock resolution.

A.1.16.2.1 Oversight of Contractor's Program Status

Reports statuses for all Contractor projects and programs within FirstNet. Status management reporting includes the reporting of milestone completions, resource utilization, and slippage and timing of deliverables to keep the project or program on track, including issue and roadblock resolution.

A.1.16.2.2 Executive and Board Reporting

Responsible for the creation, delivery, and presentation of executive summary reports of all project information, statuses, and progress reports to the FirstNet Board and executive team.

A.1.17 Sales Management Oversight and Performance Monitoring

Tracks the overall progress of sales and related activities for devices and services. Works with the Contractor to ensure sales meet or exceed targets and, if necessary, to agree on mitigation plans.

A.1.17.1 Account Planning Compliance

Monitors account planning strategy for compliance regarding sales and ongoing account management functions.

A.1.17.2 Priority Elements of Sales Strategy Identification

Identifies strategic priorities to implement the sales plans for all segments of customers and monitors the performance of sales plans.

A.1.17.3 Sales Strategy Approval

Approves the strategic framework for the successful implementation of the sales plans for all segments of customers and monitors its performance.

A.1.17.4 Sales Targets and Performance Monitoring

Develops short- and long-term sales targets and adjusts according to changing market trends and dynamics. Measures target performance achievements.

A.1.17.5 Sales Monitoring and Compliance

Develops a standard sales performance monitoring framework and ensures the timely distribution and review of sales reports.

A.1.17.6 Special Offers Approval

Reviews and approves special products, services, and pricing offers.

A.1.17.7 Pricing Strategy Agreement

Negotiates and achieves agreement with the Contractor on pricing strategies for services, features, and devices based on FirstNet's recommended pricing strategy.

A.1.17.8 User Purchasing Process Approval

Approves user purchasing processes for individually liable accounts.

A.1.18 Oversight of Contractor's Performance Related to Providing Customer Care

Oversees and monitors the Contractor's performance related to providing customer care for the NPSBN.

A.1.18.1 Resolution of Issues

Coordinates with the Contractor to collect input and needs from FirstNet stakeholders to assist in the evolution of user and technical issues.

A.1.19 Technical Oversight and Project Management

Oversees the Contractor's work as it relates to all technical project management aspects of the NPSBN.

A.1.19.1 Network Solutions End-to-End Architecture Oversight

Oversees the development of the overall end-to-end architecture of the NPSBN within each life-cycle integration.

A.1.19.1.1 Technical Project Management

Oversees the technical project management for systems engineering activities related to developing, implementing, and operating the NPSBN, as well as delivering services and managing the evolution of technologies.

A.1.19.1.1.1 Technical Schedule and Risk Management

Oversees the Contractor's technical schedule and risk management for systems engineering activities related to developing, implementing, and operating the NPSBN, as well as delivering services and managing the evolution of technologies.

A.1.19.1.1.2 Engineering and Integration Risk Management

Oversees the Contractor's performance of engineering and integration risk management for systems engineering activities related to developing, implementing, and operating the NPSBN, as well as delivering services and managing the evolution of technologies.

A.1.19.1.2 Public Safety Quality Assurance Testing at the FirstNet Laboratory

Creates and executes FirstNet's quality assurance test plans and test cases to verify the quality and functionality of public safety features. Performs cybersecurity quality assurance testing to verify that security features do not negatively impact functionality for end users. Oversee the Contractor's FirstNet acceptance test execution of public safety features. Oversees the Contractor's FirstNet cybersecurity acceptance testing to verify that security features do not negatively impact functionality for end users.

A.1.19.1.3 FirstNet Laboratory Facility Management

Manages and maintains the FirstNet laboratory facility space; power; heating, ventilation, and air conditioning (HVAC); battery backup; backup generators; external Internet Protocol (IP) connectivity; test bench furniture; standard test equipment; applicable software licenses; and end-user test devices.

A.1.19.1.4 Experience Center Facility Management

Manages and maintains the Experience Center space, power, HVAC, IP connectivity, furniture, applicable software licenses, and end-user test devices.

A.1.19.2 Technical Operations Life-Cycle Oversight

Oversees technical operations and practices within the NPSBN.

A.1.19.2.1 Systems Engineering Oversight

Oversees the systems engineering architecture, design, integration, and evolution of the NPSBN.

A.1.19.2.2 Oversight of Technology Implementation

Provides oversight of technology implementation operations and practices of the NPSBN.

A.1.19.2.3 Technology Risk Management Oversight

Oversees operations and practices related to technology risk management for the NPSBN.

A.1.19.2.4 Technology Change Management Oversight

Oversees operations and practices related to technology change management for the NPSBN.

A.1.19.2.5 Technology Configuration Management Oversight

Oversees operations and practices related to technology configuration management for the NPSBN.

A.1.19.2.6 Technology Refresh Oversight

Oversees technology evolution planning and implementation within the NPSBN.

A.1.19.2.7 Technical Review Gates

Manages all approval gates within the systems engineering life-cycle.

A.1.19.2.8 Technical Compliance Oversight for States that Assume Responsibility for Deploying the RAN

Oversees compliance of states and territories that assume responsibility for deploying their RAN with FirstNet technical policies, procedures, and architecture.

A.1.19.2.9 Provisioning Policy and Procedure Compliance

Monitors, enforces, and provides feedback on the provisioning policies and procedures implemented by the Contractor.

A.1.19.2.10 Operational Procedure Compliance

Monitors, enforces, and provides feedback to support the improvement of network operational procedures.

A.1.19.3 Technical Strategy Approval

Approves short- and long-range technical roadmaps and strategies for the NPSBN.

A.1.19.3.1 Concept Development

Provides concept development of the services and technical functionalities needed to meet public safety requirements.

A.1.19.3.1.1 Proof-of-Concept and Field Testing Participation and Approval

Tests future prototypes, including features, cybersecurity, and functionality. Ensures prototypes align with industry developments and standards and their applicability to the public safety marketplace.

A.1.19.3.2 Roadmap Development

Oversees the development of NPSBN technical roadmaps.

A.1.19.3.2.1 Public Safety Product and Feature Roadmap Approval

Approves NPSBN portfolio roadmaps to optimize the supply of products, features, and functionality to meet the evolving needs of the public safety community.

A.1.19.3.2.2 Near-Term Public Safety Product Roadmap Approval

Approves the Contractor's near-term public safety product roadmap based on input from FirstNet and the public safety community.

A.1.19.3.2.3 Outreach Feedback for Long-Term Services

Gathers feedback and requirements from the public safety community regarding outreach about the development of public safety product roadmaps that focus on three years and beyond.

A.1.19.3.2.4 Long-Term Features and Services Development

Identifies system features and services in support of the long-term public safety product roadmap.

A.1.19.3.2.5 Features and Services Integration into Long-Term NPSBN Roadmap

Provides a pre-decisional position on the integration of features and services into the long-term NPSBN roadmap.

A.1.19.3.2.6 Device Portfolio Strategy Approval

Defines the range of device/accessory types and pricing to cover all public safety service requirements.

A.1.19.3.2.7 Public Safety Standards Roadmap Development

Drives standards organizations to implement the FirstNet long-term roadmap.

A.1.19.3.2.7.1 Global and U.S. Standards Strategy Approval

Approves the Contractor's strategy and tactics for ensuring FirstNet's feature requirements are supported by applicable global anad national standards and contained in the Contractor's standards releases.

A.1.19.3.2.7.2 Tactical Participation in Global and U.S. Standards

Interfaces and coordinates with the Contractor to ensure FirstNet's feature requirements and items are supported by global and national standards bodies and included in the Contractor's standards releases.

A.1.19.3.3 Requirements Engineering Oversight

Collates product requirements to develop engineering guidelines and system requirements.

A.1.19.4 Disaster Response and Major Event Support

Oversees the Contractor's disaster response planning, training, and support of major events and disaster scenarios, driving continuous improvement.

A.1.19.4.1 Agency Support for NPSBN Mitigation Plan Development

Provides local, state, tribal, and/or federal agencies with mitigation planning support for disasters and major events, including conducting training exercises with constituents.

A.1.19.5 State Plans Oversight

Oversees the development and presentation of state plans.

A.1.19.5.1 Public Safety Stakeholder Data Collection and Analysis

Defines, collects, and analyzes state data elements—such as coverage objectives, users and operational areas, capacity planning, and training needs—for incorporation into state plans.

A.1.19.5.2 State Plan Change Management

Coordinates stakeholder inputs, requests, and engagements relative to changes in the state plans.

A.1.19.5.3 Delivery of State Plans to Governors

Consolidates state consultation/outreach data with Contractor-provided support products into a final state plan for signature by the governor of each of the 56 states and territories.

A.1.20 End-to-End Security Oversight

Oversees the development of an end-to-end network security policy, process, and procedures framework that aligns with evolving standards and prevailing conditions to meet the end-to-end security requirements outlined in Section J, Attachment J-3, FCC TAB RMTR, and Section J, Attachment J-10, Cybersecurity, as well as Section C, Statement of Objectives.

A.1.20.1 Federal Security Monitoring

Oversees the monitoring of the security posture of the NPSBN for any incidents, detected by the Contractor, that may negatively affect the confidentiality, integrity, or availability of network devices, end-user devices, and systems.

A.1.20.1.1 Cyber Incident Response Oversight

Oversees incident response to NPSBN system and user incidents and ensures the Contractor provides timely and accurate reporting, as required, as well as any required external reporting.

A.1.20.1.2 Vulnerability Management Oversight

Oversees the methodology of the Contractor to conduct and maintain routine, consistent vulnerability scanning of the NPSBN infrastructure that is passive to ensure no impact to systems. Oversees the management of efficient, effective remediation of any discovered vulnerabilities, which may include continuously applying software updates and patches to systems and equipment that reside on the NPSBN.

A.1.20.1.3 Cyber Defense Monitoring

Oversees the methodology of the Contractor to develop and deploy a defensive architecture to proactively monitor the NPSBN systems for indications of malicious activity—both internal and external. The architecture should include in-depth defense tactics and varied technologies, such as intrusion detection systems, intrusion prevention systems, net flow capture, and packet capture.

A.1.20.1.4 Policy Development and Monitoring

Develops security policies in collaboration with the public safety community and federal agencies. Provides governance and guidance on managing NPSBN cybersecurity risks. Oversees the Contractor's program to ensure end users' compliance with security policies and procedures, including security training.

A.1.20.1.5 Support for Disasters and Major Events

Provides support for disaster response and recovery and major events, including physical assets, human resources, advance planning, and execution protocols to enable rapid response. Provide cybersecurity support during disasters and major events, as necessary, to ensure they do not become a point of weakness in the network.

A.1.20.1.6 Cybersecurity Intelligence and Threat Analysis

Oversees the Contractor's cybersecurity intelligence and threat analysis processes and procedures, ensuring the implementation of cybersecurity functions in security systems based on the collection, analysis, and reporting of cybersecurity threat data and malicious activity in order to mitigate potential security breaches.

Table of Contents

List of Tables

1 Document Overview

This document provides details pertaining to the target Initial Operational Capability (IOC)/Final Operational Capability (FOC) timeline for the First Responder Network Authority (FirstNet) Nationwide Public Safety Broadband Network (NPSBN). This timeline correlates with the 3rd Generation Partnership Project (3GPP) standard body release timeline; the milestones of the corresponding NPSBN deployment are referenced herein. This document should be read in conjunction with Section B, Supplies or Services and Prices/Costs.

2 IOC/FOC Target Timeline

The IOC/FOC Target Timeline details FirstNet's objectives for deployment of various features and associated coverage milestones. As noted in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.1.1, Section One – General, and Section L.3.1.2, Section Two – Leadership and Program Management, Offerors are to propose a Performance Work Statement (PWS), a Work Breakdown Structure (WBS), and an Integrated Master Schedule that details the proposed IOC/FOC timeline.

Nationwide tasks and milestones (State Plans and Delivery Mechanism, Nationwide Coverage and Capacity Solutions, Products and Architecture, and Business Management) for IOC-1 commence with Day 1 task orders. State tasks and milestones (Public Safety Device Connections, State Coverage and Capacity Solutions, and Substantial Rural Milestones for states and territories) for IOC-2 commence with the RAN task order issuance for each state or territory.

The timing of the features and functions within the IOC/FOC timeline may be adjusted per the publication and availability of 3GPP releases and their associated features and functionalities.

The IOC-3 reference to Next Generation 9-1-1 (NG911) should take into consideration Section 4.4.6.3, NG 911 Services, from Section J, Attachment J-3, FCC TAB RMTR.

The coverage-related IOC/FOC milestones apply to persistent coverage, which satisfies the coverage requirements. Temporary coverage, such as that provided by deployable units or backpack transmitters, may be used to complement persistent coverage. However, temporary coverage does not count toward the IOC/FOC coverage deployment percentage goals.

"Completed" is defined as when all relevant components—devices, network, services, and applications—are deployed, operating, and generally available to provide end-to-end service.

Table 1 IOC/FOC Milestones

	Timing/Area	IOC-1 6 months from award	IOC-2* 12 months	IOC-3* 24 months	IOC-4* 36 months	IOC-5* 48 months	FOC* 60 months
3GPP MILESTONES							
A.	**3GPP Release**	• 3GPP Release 12 generally available		• 3GPP Release 13 generally available		• 3GPP Release 14 generally available	
NATIONWIDE MILESTONES							
B.	**State Plans and Delivery Mechanism**	• Launch of the Web interface for state plan delivery (Task Order #1) • Initiate issuance of state plans (Task Order #2)					
C.	**Coverage and Capacity Solutions (State and Territory Task Orders)**	• Nationwide coverage on Band-14 or Non Band-14 • Band 14 deployables available • Range extension services • Band 14 laboratory tests					
D.	**Products and Architecture (Task Order #3)**	• Completion of data and voice services Phase 1 • Completion of QPP	• Completion of data and voice services Phase 2 • Completion of QPP	• Completion mission-critical services, systems, and operations Phase 1	• Completion of mission-critical services, systems, and operations Phase 2	• Completion of mission-critical services, systems, and operations Phase 3	• Delivery of all IOC services, applications, infrastructure,

Timing/Area	IOC-1 6 months from award	IOC-2* 12 months	IOC-3* 24 months	IOC-4* 36 months	IOC-5* 48 months	FOC* 60 months
• Services • Applications • Devices • Architecture and Infrastructure • Operations	Phase 1 (Framework) • Completion of ICAM Phase 1 • Completion of applications ecosystem Phase 1 • Completion of local control application Phase 1 • Completion of PSE home page • Completion of devices Phase 1 • Completion of Core infrastructure Phase 1 • Completion of infrastructure hardening Phase 1 • Completion of security Phase 1 • Launch of initial network operations (Band 14 or non-Band 14) • Launch agency systems onboarding • Completion of PSEN	Phase 2 (Static QPP) • Completion of ICAM Phase 2 • Completion of applications ecosystem Phase 2 • Completion of public safety applications Phase 1 • Completion of local control application Phase 2 • Completion of devices Phase 2 • Completion of Core infrastructure Phase 2 • Completion of infrastructure hardening Phase 2 • Completion of security Phase 2 • Launch of Band 14 network operations • Launch of FirstNet operational SMC • Launch FirstNet field operations • Completion of PSEN	• Completion of QPP Phase 3 (Dynamic QPP) • Completion of applications ecosystem Phase 3 • Completion of public safety applications Phase 2 • Completion of local control application Phase 3 • Completion of devices Phase 3 • Completion of Core infrastructure Phase 3 • Completion of infrastructure hardening Phase 3 • Completion of security Phase 3 • Completion of PSEN onboarding and interconnection Phase 3 • Completion of RF site integration to Core Phase 2	• Completion of location-based service enhancements • Evolve systems, services, and devices to meet growth and feature enhancements • Completion of Core infrastructure Phase 4 • Completion of infrastructure hardening Phase 4 • Completion of security Phase 4 • Completion of PSEN onboarding and interconnection Phase 4 • Completion of RF site integration to Core Phase 3	• Completion of Core infrastructure Phase 5 • Completion of infrastructure hardening Phase 5 • Completion of security Phase 5 • Completion of PSEN onboarding and interconnection Phase 5 • Completion of RF site integration to Core Phase 4	and operations milestones to meet FOC objectives • Satisfaction of evolution and roadmap development milestones and objectives • Satisfaction of PSEN integration objectives • Satisfaction of RF site integrations to Core objectives • Satisfaction of operational objectives

	Timing/Area	IOC-1 6 months from award	IOC-2* 12 months	IOC-3* 24 months	IOC-4* 36 months	IOC-5* 48 months	FOC* 60 months
		onboarding and interconnection Phase 1 • Completion of non-Band 14 public safety user migration Phase 1 • Completion of non-Band 14 network operations	onboarding and interconnection Phase 2 • Completion of RF site integration to Core Phase 1 • Completion of non-Band 14 public safety user migration Phase 2				
E.	**Business Management (Task Order #3)**	• Implement CRM, sales, billing, and financials utilizing existing business support systems	• Complete CRM, sales, billing, and financial business support systems specific to FirstNet	• Evolution of business support systems to meet growth and feature enhancements			• Completion of business support systems deployment and operational milestones
STATE MILESTONES							
F.	**Public Safety Device Connections**			• Achievement of 50% of Contractor's IOC-5 public safety device connections target		• Achievement of 100% of Contractor's public safety device connections target	

	Timing/Area	IOC-1 6 months from award	IOC-2* 12 months	IOC-3* 24 months	IOC-4* 36 months	IOC-5* 48 months	FOC* 60 months
G.	**Coverage and Capacity Solutions (State and Territory Task Orders)**		• Achievement of 20% of Contractor's proposed Band 14 coverage in non-rural areas	• Achievement of 60% of Contractor's proposed Band 14 coverage in non-rural areas	• Achievement of 80% of Contractor's proposed Band 14 coverage in non-rural areas	• Achievement of 95% of Contractor's proposed Band 14 coverage in non-rural areas	• Achievement of 100% of Contractor's proposed Band 14 coverage in non-rural areas
H.	**Substantial Rural Milestones (State and Territory Task Orders)**		• Achievement of 20% of Contractor's proposed Band 14 coverage in rural areas	• Achievement of 60% of Contractor's proposed Band 14 coverage in rural areas	• Achievement of 80% of Contractor's proposed Band 14 coverage in rural areas	• Achievement of 95% of Contractor's proposed Band 14 coverage in rural areas	• Achievement of 100% of Contractor's proposed Band 14 coverage in rural areas

* Timeframes listed represent months from actual award date (subsequent task orders)

3 Timeline Details

3.1 IOC-1

IOC-1 is targeted to occur within the first six (6) months post contract award. The initial launch of the NPSBN may use existing wireless services branded as "FirstNet," similar to a Mobile Virtual Network Operator (MVNO) implementation. These milestones are targeted to align with the availability and implementation of 3GPP releases.

The NPSBN features and functions that are targeted to be available during this phase follow.

3.1.1 IOC-1 – State Plans and Delivery Mechanism

IOC-1 includes the development of state plans as well as an online tool for their delivery. See Sectio

1. **Launch the Delivery Mechanism for State Plans (Task Order #1)** – Web interface tool to deliver state plans for each of the 56 states and territories. See Section F, Deliverables and Performance, F.2.1.1, Delivery Mechanism for State Plans.
2. **Complete and Issue All State Plans (Task Order #2) –** See Section F, Deliverables and Performance, F.2.1.2, State Plan Development and Refinement.

3.1.2 IOC-1 – Coverage and Capacity Solutions (State and Territory Task Orders)

Coverage and capacity solutions for IOC-1 should provide nationwide coverage through existing wireless service (e.g., MVNO non-Band 14) deployments. Band 14 deployable units and range extension technologies are required to address possible coverage deficiencies and public safety emergencies. The following coverage solutions shall be tested before deployment:

1. Nationwide coverage using currently available wireless services
2. Vehicular Network Systems (VNSs), formerly called the Mobile Communications Units or MCUs
    a. Testing should ensure general availability of VNSs are certified for performance and reliability and ready for deployment.
    b. Installation instructions and collateral shall be provided to certified installation vendors.
3. Available Band 14 deployable units, including VNSs
4. Range extension services (e.g., satellite services, high-power User Equipment support)
5. Band 14 laboratory trials shall be conducted for products and services unique to public safety.

3.1.3 IOC-1 – Products and Architecture

Products and architecture for IOC-1 cover all services, applications, devices, architecture and infrastructure, and operations required to meet initial FirstNet non-Band 14 coverage objectives. During this phase, the Contractor shall initiate NPSBN implementation to prepare for integration with state-deployed Radio Access Network (RAN) systems and new site builds.

3.1.3.1 Services

Services for IOC-1 cover all FirstNet network services and enabler milestones required to meet initial non-Band 14 coverage objectives. During this phase, the Contractor shall complete the services and enablers of the Core in preparation for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Data and Voice Services Phase 1**
    a. Long Term Evolution (LTE)/4G consumer grade data in all coverage areas
    b. LTE/4G consumer video service in all coverage areas
    c. LTE/4G consumer grade messaging in all coverage areas
    d. LTE consumer grade Voice over LTE (VoLTE) and voice in all coverage areas
    e. Voice fall back to commercial voice services where VoLTE is unavailable
    f. Consumer grade streaming video in all coverage areas
    g. Roaming to other commercial networks using the Contractor's network roaming agreements in areas where FirstNet coverage is unavailable. All services are available on roaming network
    h. Basic location-based service support in all coverage areas
    i. Wireless Emergency Alerts (WEA) in all coverage areas
    j. Lawful Interception (LI) in all coverage areas
    k. Phase II 9-1-1 services in all coverage areas
2. **Complete Quality of Service, Priority, and Preemption (QPP) Phase 1 (Framework)**
    a. Use of LTE prioritization capabilities to define public safety QPP profiles
    b. QPP framework that provides interoperability to ensure end-to-end priority capabilities across network partner(s) and Band 14
    c. End-to-end priority for public safety users
    d. Priority treatment for roaming public safety users
    e. Overload control or other mechanisms to ensure end-to-end priority for public safety users even when the network experiences congestion
    f. End-to-end Quality of Service (QoS) integrity and interworking with mobile Virtual Private Network (mVPN) solutions employed by Public Safety Enterprise Networks (PSENs).
3. **Complete Identity, Credential, and Access Management (ICAM) Phase 1**
    a. ICAM interoperability defined
    b. User attribute interoperability definition for Attribute-Based Access Control (ABAC)
    c. Onboarding of early adopter public safety agencies into ICAM trust framework
    d. Agency identity proofing process defined and implemented
    e. Hosted identity solution for public safety agencies that choose not to implement their own identity provider for user authentication
    f. Federated identity management for early adopters leveraging the defined ICAM trust framework
    g. Single Sign-On (SSO) for mobile devices

3.1.3.2 Applications

During IOC-1, the Contractor shall implement and deploy an applications ecosystem that consists of a FirstNet applications store featuring applications specific to public safety, hosted cloud services, an application developer's ecosystem, and a Service Delivery Platform and associated Application Programming Interfaces (APIs), as defined in the architecture, design, and implementation plans. The Contractor shall define the processes and procedures for public safety agencies and third parties to use the applications ecosystem and for public safety agencies and developers to use the application developer's ecosystem to produce certified Public Safety Grade applications. Specific milestones include the following:

1. **Complete Applications Ecosystem Phase 1**
    a. FirstNet applications store for public safety applications
    b. Certified public safety applications available to public safety users from both the FirstNet applications store and commercial applications stores
    c. Hosted cloud services offered to public safety agencies and application developers, including Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS)
    d. User, data, and service analytics and analytic services/APIs
    e. Application's developer ecosystem, including developer Web page, Mobile Application Development Platform (MADP), software developer kits (SDKs), and developers' tools
    f. Application and developer certification process and requirements defined
    g. Application certification environment available
    h. Service Delivery Platform framework integration for FirstNet that includes middleware and back-end network services integration
    i. APIs and SDKs available for federated ICAM, including securely accessing local, state, regional, tribal, and federal databases and resources
    j. APIs and SDKs available for delivered network services
    k. APIs and SDKs available for SSO on mobile devices
2. **Complete Local Control Application Phase 1**
    a. Agency local control administration and management application utilizing existing online systems
    b. Agencies able to manage agency accounts and subscriptions
    c. Agencies able to manage users, groups, and basic profiles
    d. Agencies able to manage devices and basic profiles
    e. Agencies able to manage applications
3. **Complete Public Safety Entity (PSE) Home Page**
    a. PSE home page available for public safety agency adoption
    b. Status of the NPSBN
    c. Situational awareness and incident information for agencies
    d. Support for local agency customization

3.1.3.3 Devices

The Contractor shall develop and provide a suitable portfolio, roadmap, and device approval process for devices made available to public safety users. Devices shall comprise commercial off-the-shelf (COTS) non-Band 14 and Band 14 enabled devices, accessories, machine-to-machine (M2M), and other specialized devices. The Contractor shall establish processes and procedures to allow an agency to deploy a Bring-Your-Own-Device (BYOD) approach on the network. Specific milestones include the following:

1. **Complete Devices Phase 1**
    a. Portfolio of COTS non-Band 14 devices suitable for public safety users and devices that can be used as BYOD to access public safety applications
    b. Portfolio and roadmap of available and planned Band 14 devices, including the following:
        i. Portables (i.e., smartphones, tablets, and modems)
        ii. In-vehicle routers

iii. Specialized devices (e.g., ruggedized, high-power, dual mode LTE/Land Mobile Radio [LMR])
iv. M2M
v. Accessories (e.g., rugged cases, battery packs, headsets)

c. FirstNet device approval process and Device Independent Verification and Validation (DIV&V) tests
d. FirstNet Universal Integrated Circuit Card (UICC) profile and common embedded applications (e.g., enablers for computer-aided dispatch, mapping, virtual assistant and voice control clients, securing devices)

3.1.3.4 Architecture and Infrastructure

Architecture and infrastructure for IOC-1 covers all Core related milestones required to meet initial FirstNet coverage objectives. During this phase, the Contractor shall commence building of the Core to prepare for integration with state-deployed RANs and new site builds, as defined in the architecture, design, and implementation plans. Specific milestones include the following:

1. **Complete Core Infrastructure Phase 1**
   a. Core systems that support non-Band 14 services are completed and ready for service, including Core Evolved Packet Core (EPC), service provisioning, and management
   b. Operational and acceptance testing of associated non-Band 14 Core systems, services, and equipment to ensure the implementation plan and RAN coverage objectives are met
   c. Begin implementation of dedicated FirstNet Core and associated subsystems.
2. **Complete Infrastructure Hardening Phase 1**
   a. Completed planned Core hardening, including:
      i. EPC hardening
      ii. Transmission systems hardening
      iii. Operational support system (OSS) hardening
      iv. Business support system (BSS) hardening
3. **Complete Security Phase 1**
   a. Basic security services provided, including:
      i. Over-the-air authentication, encryption, and integrity protection
      ii. Data management from a device and ability to disable the device in case of a security breach
      iii. Secure connections between eNodeBs and the Core with the ability to pass mVPN services and interwork with LTE Grade Of Service (GOS)
      iv. Firewalls and intrusion protection services to secure traffic between the Core network and external networks, creating a trusted network infrastructure
   b. Complete implementation of subscriber database management for security and management
   c. Support for the transport of secure data services in conjunction with application-level Transport Socket Layer (TSL) and other device-to-application security connection methods
   d. Launch of network monitoring and security event tracking

3.1.3.5 Operations

Operations for IOC-1 cover all network operations milestones required to meet initial FirstNet coverage objectives. During this phase, the Contractor shall initiate building of the Core to prepare for state-deployed RANs and new site builds. Specific milestones include the following:

1. **Commence Non-Band 14 Network Operations**
    a. Network operations processes and procedures are implemented and support organizations are in place and fully resourced, operational, and able to monitor non-Band 14 system(s)
    b. Fully operational Services Management Center (SMC) that can monitor non-Band 14 systems
    c. Performance metrics tracked, monitored, corrected, and reported
    d. OSS connected and synchronized with local control system to provide network statistics and performance of non-Band 14 system(s)
    e. Public safety Open Mobile Alliance Device Management (OMA-DM) policies and OMA-DM for non-Band 14 service provisioning
2. **Launch Agency Systems Onboarding**
    a. Integrated device ordering and provisioning systems with FirstNet-branded, customer-facing Web portal
    b. Operational device distribution channels
    c. Packaging specification for device types provided to distributors
    d. Integrated partner solution with local agency asset systems
3. **Complete PSEN Onboarding and Interconnection Phase 1**
    a. Implementation plan for integrating each PSEN into the NPSBN, which includes methods, milestones, and a timeline to establish PSEN point-of-presence locations; implement PSEN connectivity and interfaces with the Emergency Services IP network (ESInet); assign APNs; and interconnect with computer-aided dispatch, dispatch, Public Safety Answering Points, and NG911 systems.
4. **Complete Non-Band 14 Public Safety User Migration Phase 1**
    a. Public safety user migration from existing wireless systems to the Core network and systems.

3.1.4 IOC-1 – Business Management

The Contractor shall implement initial business management services using Contractor-provided BSS.

1. **Implement Customer Relationship Management (CRM), Sales, Billing, and Financials Utilizing Existing Business Support Systems**
    a. Business support systems for sales planning, sales forecasting, monitoring, tracking and compliance, sales operations, sales training, and compensation
    b. Business support systems for billing, account management, asset tracking, and financials

3.2 IOC-2

IOC-2 is targeted to occur within one (1) year post contract award. In addition to the features and functionalities targeted to be available at the launch of the NPSBN, the following features and functionalities are targeted to be available.

3.2.1 IOC-2 – Coverage and Capacity Solutions

Deployment of Band 14 coverage solutions for both rural and non-rural areas begins in IOC-2.

1. **Non-rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)
2. **Rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)

3.2.2 IOC-2 – Products and Architecture

Products and architecture for IOC-2 cover all services, applications, devices, architecture and infrastructure, and operations required to meet initial FirstNet coverage objectives. During this phase, the Contractor shall prepare the NPSBN and for integration with state-deployed RANs and new site builds.

3.2.2.1 Services

Services for IOC-2 cover all FirstNet network services and enabler milestones required to meet initial FirstNet coverage objectives. During this phase, the Contractor shall complete the services and enablers of the Core in preparation for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Data and Voice Services Phase 2**
    a. Data on Band 14 deployments and interworking with non-Band 14 systems and services
    b. Video service and messaging on Band 14 deployments and interworking with non-Band 14 systems and services
    c. VoLTE on Band 14 deployments and interworking with non-Band 14 systems and services
    d. Multicast video
    e. Consumer-grade Push-to-Talk (PTT)
    f. Begin FirstNet location-based services
    g. FirstNet WEA
    h. FirstNet LI
    i. FirstNet 9-1-1
    j. FirstNet Evolved Multimedia Broadcast Multicast Service (eMBMS)
2. **Complete QPP Phase 2 (Static QPP)**
    a. FirstNet QPP framework for voice, video, guaranteed bit rate (GBR) data, and non-GBR data services in Band 14
    b. System to check user credentials for priority services and map users to their default QPP profiles
    c. Defined QPP framework for Band 14 that interoperates and aligns with the Contractor's network priority services
    d. Pre-emption profiles and interoperability with priority settings
3. **Complete ICAM Phase 2**
    a. Enhancements to FirstNet trust framework (ICAM, user attribute definitions, and new capabilities)
    b. Onboarding of PSEs
    c. General availability of federated access for participating agencies to local, state, regional, tribal, and federal applications, services, databases, and resources
    d. ICAM solution in all Contractor-provided applications

3.2.2.2 Applications

The Contractor shall enhance the applications ecosystem and application developer's ecosystem to incorporate new network services, APIs and SDKs, innovations, and general updates, including local control updates for static QPP. Specific milestones include the following:

1. **Complete Applications Ecosystem Phase 2**
    a. APIs and SDKs available for interacting with static QPP network service
    b. APIs and SDKs available for new network services
    c. Enhancements to Service Delivery Platform, application developer's ecosystem, FirstNet applications store, and cloud services
2. **Complete Public Safety Applications Phase 1**
    a. Third-party applications leveraging static QPP APIs
    b. Applications evolution and continuous delivery based on public safety feedback, needs, and technology innovations
3. **Complete Local Control Application Phase 2**
    a. Ability to control/manage static QPP via local control
    b. Public Safety Enterprise (PSE) home page application evolution and continuous delivery

3.2.2.3 Devices

The Contractor shall update the portfolio of devices for public safety with new devices from Original Equipment Manufacturers (OEMs) that are suitable for the NPSBN and aligned with agencies' expectations. Upon publication of 3GPP release 12, the Contractor shall provide updated software-related packaging details to distributor(s) of all affected device types, features, and embedded applications. In addition, the Contractor shall provide software and firmware update release schedules in accordance with network software updates. Specific milestones include the following:

1. **Complete Devices Phase 2**
    a. Portfolio of Band 14 devices across all categories
    b. Devices certified for safety through FirstNet DIV&V testing

3.2.2.4 Architecture and Infrastructure

Architecture and infrastructure for IOC-2 covers all Core milestones required to meet FirstNet coverage objectives. During this phase, the Contractor shall finish building the Core to prepare for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Core Infrastructure Phase 2**
    a. Core is online and in use
    b. Equipment orders, deliveries, deployments, and operational acceptance for the Core services and resources to meet the implementation plan delivery milestones to ensure RAN coverage objectives are met
    c. Implementation of architected Core to ensure the network is ready for acceptance and integration with state-deployed RANs and new build sites
        i. On-Network QoS (infrastructure and device) on Band 14 deployments and interworking with non-Band 14 systems
        ii. Inclusion of Mobile Management Entity (MME), Serving Gateway/Packet Data Network Gateway (S/PGW), Home Subscriber Server (HSS), Policy and

Changing Rules Function (PCRF), IP Multimedia Subsystem, Session Description Protocol, Diameter Routing Agent (DRA), OSS, BSS, routers, switches, firewalls, transmission systems, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHSCP), and Intrusion Detection System (IDS) in Core systems

iii. Contractor's 3G network interworking with Band 14 coverage

2. **Complete Infrastructure Hardening Phase 2**
    a. Core hardening, including for state-deployed RANs and new site builds
        i. Core redundancy and failover to meet availability objectives
        ii. Geo-redundancy and failover to meet availability objectives
        iii. Geo-diverse transport to meet availability objectives
3. **Complete Security Phase 2**
    a. Security mechanisms for the applications ecosystem
        i. Consistency checks to mitigate spoofing of applications to devices
        ii. Integrity validation to ensure legitimacy of downloads
    b. Enhanced monitoring of network traffic and security events
        i. Band 14 sites
        ii. Non-Band 14 sites
        iii. Applications

3.2.2.5 Operations

Operations for IOC-2 cover all network operations milestones required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete and perform acceptance testing for the Core and for new site builds. Specific milestones include the following:

1. **Commence Band 14 Operations**
    a. OMA-DM for Band 14 service provisioning
2. **Commence FirstNet Operational SMC**
    a. Methods and procedures for all operational activities, resources, and structures (e.g., change management)
    b. Active, support systems that are populated with appropriate data and work flows
    c. Operational resources and structures
3. **Commence FirstNet Operations**
    a. Methods and procedures for all operational activities, resources, and structures (e.g., change management)
    b. Active, operational support systems that are populated with appropriate data and workflows
    c. Operational resources and structures
4. **Complete PSEN Onboarding and Interconnection Phase 2**
    a. Integrate additional PSEN sites based PSEN onboarding implementation plan.
    b. Accommodation of Over-the-Top (OTT)-based PTT until standards-based Mission Critical (MC)-PTT is available.
    c. Tested and verified end-to-end bearer encryption and local use of mVPN solutions interworking in conjunction with FirstNet QoS
5. **Complete Radio Frequency (RF) Site Integration to Core Phase 1**
    a. Completed RF site integration and on-air acceptance tests

b. Transfer to operations for associated state-deployed RANs, Band 14 and non-Band 14 RANs, services, and equipment

6. **Complete Non-Band 14 Public Safety User Migration Phase 2**
   a. Migration of public safety users from existing wireless systems to the FirstNet Core and systems

3.2.3 IOC-2 – Business Management

The Contractor shall establish business management systems and services specifically for the NPSBN, including CRM, sales, billing, and financial systems.

1. **Complete CRM, Sales, Billing and Financial Business Support Systems Specific to FirstNet**
   a. CRM systems and tools to support marketing, help desk, point of sale of FirstNet devices, services, and reporting on Key Performance Indicators
   b. Form and functionality of a FirstNet-branded customer-facing Web portal that allows agencies to view and order devices, service offerings, and accessories
   c. BSS for sales planning; sales forecasting, monitoring, tracking, and compliance; sales operations; sales training; and compensation.
   d. BSS for billing, account management, asset tracking, and financials

3.3 IOC-3

IOC-3 is targeted to occur within two (2) years post contract award. In addition to the features and functionalities targeted to be available at IOC-2, the following features and functionalities are targeted to be available.

3.3.1 IOC-3 – Coverage and Capacity Solutions

IOC-3 coverage solutions significantly expand non-rural and rural Band 14 coverage.

1. **Non-rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)
2. **Rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)

3.3.2 IOC-3 – Products and Architecture

Products and architecture for IOC-3 cover all services, applications, devices, architecture and infrastructure, and operations required to meet FirstNet coverage objectives. During this phase, the Contractor shall complete the NPSBN and prepare for integration with state-deployed RANs and new site builds.

3.3.2.1 Services

Services for IOC-3 cover all FirstNet network services and enabler milestones required to meet FirstNet coverage objectives. During this phase, the Contractor shall complete the services and enablers of the Core in preparation for integration with state-deployed RANs and new site builds as defined in the architecture, design, and implementation plans. Specific milestones include the following:

1. **Complete Mission-Critical Services, Systems, and Operations Phase 1**
   a. Enhanced messaging
   b. Enhanced Band 14 LTE Public Safety Grade VoLTE
   c. MC-PTT
   d. Multi-cast service (eMBMS)
   e. Multi-cast WEA

f. Group Communication System Enablers (GCSE)
g. Proximity Services (ProSe)

2. **Complete QPP Phase 3 (Dynamic QPP)**
   a. Ability to invoke emergency priority treatment for public safety users
   b. Configured NPSBN elements that support dynamic QPP on Band 14, including pre-emption

3.3.2.2 Applications

The Contractor shall update the applications ecosystem, local control application, PSE home page, and default applications. Specific milestones include the following:

1. **Complete Application Ecosystem Phase 3**
   a. Steady stream of new third-party public safety applications being developed, certified, and published to the FirstNet applications store
   b. APIs and SDKs available for interacting with dynamic QPP network service
   c. APIs and SDKs available for newly delivered network services
   d. Continued enhancements to Service Delivery Platform, application developer's ecosystem, FirstNet applications store, and cloud services
2. **Complete Public Safety Applications Phase 2**
   a. Third-party applications that leverage dynamic QPP APIs
   b. Applications evolution and continuous delivery based on public safety needs, feedback, and technology innovations
3. **Complete Local Control Application Phase 3**
   a. Local control systems that support dynamic QPP
   b. Ability to control/manage dynamic QPP via local control
   c. PSE home page application evolution and continuous delivery based on public safety needs, feedback, and technology innovations

3.3.2.3 Devices

The Contractor shall update the portfolio of devices for public safety with new devices from OEMs that are suitable for the NPSBN and align with agencies' expectations. Upon publication of 3GPP release 13, the Contractor shall test, validate, and release new public safety features, including MC services, for general availability across the NPSBN. The Contractor shall make virtual assistant services unique to public safety generally available; these services shall include discipline-specific languages and commands and utilize segregated (non-commercial) servers and storage. The Contractor shall provide software and firmware update release schedules in accordance with network software updates. Specific milestones include the following:

1. **Complete Devices Phase 3**
   a. **Band 14 Device Portfolio Available** – Make additional Band 14 enabled devices available across all categories to PSEs.
   b. **Devices are safe for network** as deemed by FirstNet's DIV&V testing.

3.3.2.4 Architecture and Infrastructure

Architecture and infrastructure for IOC-3 covers all Core milestones required to meet FirstNet coverage objectives. During this phase, the Contractor shall complete additions to the Core to prepare for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Core Infrastructure Phase 3**
    a. Core additions for state-deployed RANs
    b. Core additions based on the overall coverage design objectives
2. Equipment orders, deliveries, deployments, and operational acceptance for the Core services and resources to meet the implementation plan delivery milestones to ensure RAN coverage objectives are met
3. **Complete Infrastructure Hardening Phase 3**
    a. Additions to Core hardening, including for state-deployed RANs
        i. Core redundancy and failover to meet availability objectives
        ii. Geo-redundancy and failover to meet availability objectives
        iii. Geo-diverse transport to meet availability objectives
4. **Complete Security Phase 3**
    a. Additional security services for deployable units
    b. Updated security services for the applications ecosystem
    c. Continuous improvement of monitoring of network traffic, tracking, and response for security events

3.3.2.5 Operations

Operations for IOC-3 cover all network operations milestones required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete final acceptance of the Core to prepare for integration with state-deployed RANs, complete final acceptance of new site builds, and PSEN onboarding activities. Specific milestones include the following:

1. **Complete PSEN Onboarding and Interconnection Phase 3**
    a. Integrate additional PSEN sites based PSEN onboarding implementation plan
    b. Support for NG911 systems
2. **Complete RF Site Integration to Core Phase 2**
    a. Completed RF site integration and on-air acceptance tests
    b. Transfer of associated state-deployed, Band 14, and non-Band 14 RANs to operations to meet coverage objectives

3.3.3 IOC-3 – Business Management

The Contractor shall enhance the NPSBN's BSS, including the CRM system and customer-facing Web portal, to scale and add features.

3.3.4 IOC-3 – State Public Safety Device Connections

The Contractor shall meet 50 percent of the IOC-5 public safety device connections target.

3.4 IOC-4

IOC-4 is targeted to occur within three (3) years post contract award. In addition to the features and functionalities targeted to be available at IOC-3, the following features and functionalities are targeted to be available.

3.4.1 IOC-4 – Coverage and Capacity Solutions

IOC-4 coverage solutions shall continue to expand non-rural and rural Band 14 coverage.

1. **Non-rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)
2. **Rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)

3.4.2 IOC-4 – Products and Architecture

Products and architecture for IOC-4 cover all services, applications, devices, architecture and infrastructure, and operations required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete the NPSBN and prepare for integration with state-deployed RANs and new site builds.

3.4.2.1 Services

Services for IOC-3 cover all FirstNet network services and enabler milestones required to meet FirstNet coverage objectives. During this phase, the Contractor shall complete the services and enablers of the Core in preparation for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Mission-Critical Services, Systems, and Operations Phase 2**
    a. MC-PTT enhancements
    b. GCSE enhancements and Single-Cell Point-to-Multipoint (SC-PTM)
    c. ProSe enhancements
    d. MC-Video
2. **Complete Location-Based Service Enhancements**

3.4.2.2 Applications

The Contractor shall update the applications ecosystem, local control application, and PSE home page. The application developer's ecosystem shall include updates to SDKs and APIs for newly provided network services.

3.4.2.3 Devices

The Contractor shall update the device roadmap with new public safety related devices from OEMs that are suitable for the NPSBN and align with agencies' expectations. Upon publication of 3GPP release 13, the Contractor shall provide updated software related packaging details to distributor(s) of all effected device types. The Contractor shall provide software and firmware update release schedules in accordance with network software updates.

3.4.2.4 Architecture and Infrastructure

Architecture and infrastructure for IOC-4 covers all Core milestones required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete additions to the Core to prepare for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Core Infrastructure Phase 4**
    a. Core additions for state-deployed RANs
    b. Core additions based on the overall coverage design objectives
2. Equipment orders, deliveries, deployments, and operational acceptance for the Core services and resources to meet the implementation plan delivery milestones to ensure RAN coverage objectives are met
3. **Complete Infrastructure Hardening Phase 4**
    a. Core hardening additions for state-deployed RAN systems
        i. Core redundancy and failover to meet availability objectives
        ii. Geo-redundancy and failover to meet availability objectives
        iii. Geo-diverse transport to meet availability objectives

4. **Complete Security Phase 4**
    a. Reviewed and updated security services to reflect technology and threat changes
    b. Security updates according to 3GPP release schedule

3.4.2.5 Operations

Operations for IOC-4 cover all network operations milestones required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete the integration of state-deployed RANs and new site builds and perform acceptance testing and continue with PSEN onboarding activities. Specific milestones include the following:

1. **Complete PSEN Onboarding and Interconnection Phase 4**
    a. Integrate additional PSEN sites based PSEN onboarding implementation plan
2. **Complete RF Site Integration to Core Phase 3**
    a. Completed RF site integrations and on-air acceptance tests
    b. Transfer of associated state-deployed, Band 14, and non-Band 14 RANs to operations to meet coverage objectives

3.4.3 IOC-4 – Business Management

The Contractor shall enhance the NPSBN's BSS, including the CRM system and customer-facing Web portal, to scale and add features.

3.5 IOC-5

IOC-5 is targeted to occur within four (4) years post contract award. In addition to the features and functionalities targeted to be available at IOC-4, the following features and functionalities are targeted to be available:

3.5.1 IOC-5 – Coverage and Capacity Solutions

IOC-5 coverage solutions shall continue to expand non-rural and rural Band 14 coverage, including coverage for all major highways.

1. **Non-rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)
2. **Rural coverage milestone met** (as noted in Table 1 IOC/FOC Milestones above)

3.5.2 IOC-5 – Products and Architecture

Products and architecture for IOC-5 cover all services, applications, devices, architecture and infrastructure, and operations required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete the NPSBN and prepare for integration with state-deployed RANs and new site builds.

3.5.2.1 Services

Services for IOC-5 cover all FirstNet network services and enabler milestones required to meet FirstNet coverage objectives. During this phase, the Contractor shall complete the services and enablers of the Core in preparation for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Mission-Critical Services, Systems, and Operations Phase 3**
    a. MC video and data
    b. MC-PTT enhancements

c. Enhanced group communications
d. Enhanced ProSe
e. Enhanced location capabilities for indoor and outdoor emergency communications

3.5.2.2 Applications

The Contractor shall update the applications ecosystem, local control application, and PSE home page. Updates to the application developer's ecosystem shall include SDKs and APIs for newly provided network services.

3.5.2.3 Devices

The Contractor shall update the portfolio roadmap for public safety with new devices from OEMs that are suitable for the NPSBN and align with agencies' expectations. The Contractor shall test, validate, certify, and release public safety features of 3GPP release 14—including MC-video and data—for general availability across the NPSBN. The Contractor shall provide software and firmware update release schedules in accordance with network software updates.

3.5.2.4 Architecture and Infrastructure

Architecture and infrastructure for IOC-5 covers all Core milestones required to meet initial FirstNet coverage objectives. During this phase, the Contractor shall complete additions to the Core to prepare for integration with state-deployed RANs and new site builds. Specific milestones include the following:

1. **Complete Core Infrastructure Phase 5**
    a. Core additions for state-deployed RANs
    b. Core additions based on the overall coverage design objectives
2. Equipment orders, deliveries, deployments, and operational acceptance for the Core services and resources to meet the implementation plan delivery milestones to ensure RAN coverage objectives are met
3. **Complete Infrastructure Hardening Phase 5**
    a. Core hardening additions for state-deployed RAN systems and growth
        i. Core redundancy and failover to meet availability objectives
        ii. Geo-redundancy and failover to meet availability objectives
        iii. Geo-diverse transport to meet availability objectives
4. **Complete Security Phase 5**
    a. Reviewed and updated existing security services to reflect technology and threat changes
    b. Security updates according to the 3GPPrelease schedule

3.5.2.5 Operations

Operations for IOC-5 cover all network operations milestones required to meet ongoing FirstNet coverage objectives. During this phase, the Contractor shall complete and perform acceptance testing efforts to integrate state-deployed RANs and new site builds, and conduct PSEN onboarding activities. Specific milestones include the following:

1. **Complete PSEN Onboarding and Interconnection Phase 5**
    a. Integrate additional PSEN sites based PSEN onboarding implementation plan
2. **Complete RF site integration to Core Phase 4**
    a. Completed RF site integrations and on-air acceptance tests

b. Transfer of associated state-deployed, Band 14, and non-Band 14 RANs to operations RANs to meet coverage objectives

3.5.3 IOC-5 – Business Management

The Contractor shall enhance the NPSBN's BSS, including the CRM system and customer-facing Web portal, to scale and add features.

3.5.4 IOC-5 – State Public Safety Device Connections

The Contractor shall meet 100 percent of the IOC-5 public safety device connections target.

3.6 FOC

FOC is targeted to occur within five (5) years post contract award to include the delivery of all milestones, services, systems, and hardening.

3.6.1 FOC – Coverage and Capacity Solutions

FOC for coverage and capacity solutions includes all milestones related to non-Band 14 and Band 14 for rural and non-rural areas that were agreed upon and approved to meet FOC objectives.

1. **All non-rural coverage milestones met** (as noted in Table 1 IOC/FOC Milestones above)
2. **All rural coverage milestones met** (as noted in Table 1 IOC/FOC Milestones above)

3.6.2 FOC – Products and Architecture

FOC for products and architecture identifies the point where all IOC objectives are met to create the initial fully functional NPSBN, which provides all the services, applications, devices, architecture and infrastructure, and operations that first responders need.

3.6.2.1 Services

FOC for services includes all deliverables and milestones related to services and service enablers.

1. The Contractor shall deliver all IOC services milestones to meet FOC objectives.
2. The Contractor shall meet roadmap development milestones and objectives.

3.6.2.2 Applications

FOC for applications includes all deliverables and milestones related to applications.

1. The Contractor shall deliver all IOC applications milestones to meet FOC objectives.
2. The Contractor shall meet roadmap development milestones and objectives.

3.6.2.3 Devices

FOC for devices includes all deliverables and milestones related to devices.

1. The Contractor shall deliver all IOC device milestones to meet FOC objectives.
2. The Contractor shall continue to evolve the devices portfolio based on approved and agreed upon roadmaps.

3.6.2.4 Architecture and Infrastructure

FOC for architecture and infrastructure includes all deliverables and milestones related to architecture, as well as all infrastructure implementation, system delivery, turn up, and acceptance of systems.

1. The Contractor shall deliver all IOC architecture and infrastructure milestones to meet FOC objectives.
2. The Contractor shall meet roadmap development milestones and objectives.

3.6.2.5 Operations

FOC for deliverables and milestones related to operations, including the integration of PSENs, state-deployed RANs, and new build sites. This also establishes all ongoing objectives conformance as well as new quality improvement objectives.

1. The Contractor shall deliver all IOC operations milestones to meet FOC objectives.
2. The Contractor shall meet roadmap development milestones and objectives.
3. The Contractor shall meet PSEN integration objectives.
4. The Contractor shall meet objectives related to RF site integrations to the Core.
5. The Contractor shall meet operational objectives.

3.6.3 FOC – Business Management

FOC for business management includes the deployment of all BSS—such as sales, customer care, and financial sustainability—that were agreed upon and approved to meet FOC objectives.

1. The Contractor shall meet milestones related to BSS deployment and operations.

4 Additional Features

Beyond the features and functions targeted within this timeline, FirstNet intends for the coverage, services, system, and hardening to evolve to meet public safety users' needs while keeping up with new technologies.

Table of Contents

List of Tables

1 Quality Assurance Surveillance Plan Matrix Template

The Offeror should include a Quality Assurance Surveillance Plan (QASP) in their response, detailing the performance metrics/standards they will provide in the form of QASP elements. Proposed performance metrics/standards should align with the deliverables specified in the Offeror's proposed Deliverables Table. When developing the QASP, the Offeror should be attentive to the First Responder Network Authority's (FirstNet) objectives as defined in Section C, Statement of Objectives (SOO).

The QASP should include but is not limited to a QASP Surveillance Matrix. Table 1 Format of QASP Surveillance Matrix provides a template and instructions for Offerors to follow when developing their QASP Surveillance Matrix. Table 2 Example of a QASP Element provides a sample version of a QASP element for reference.

Table 1 Format of QASP Surveillance Matrix

QASP ID #	Purpose	Performance Standard	Acceptable Performance Level	Method of Surveillance	Measures/ Metrics	Performance Target	Calculation/ Formulas	Reference SOO Objective
Provide a unique ID label	Describe the desired objective of the performance standard	Provide a short description of the performance standard	Provide, using a quantifiable and measurable metric, a definition for achieving acceptable performance of the performance standard	List the methods of surveillance to be used and the frequency of occurrence	Provide a detailed description of how the performance standard will be measured	Relate the measurement described in the Measures/ Metrics column to the four (4) performance rating levels of described in Section J, Attachment J-6, Quality Assurance Surveillance Plan	Provide a detailed description of how values defined in the Measures/ Metrics column are calculated	List correspon ding objectives from the SOO that this performan ce standard intends to address

Table 2 Example of a QASP Element

QASP ID #	Purpose	Performance Standard	Acceptable Performance Level	Method of Surveillance	Measures/ Metrics	Performance Target	Calculation/ Formulas	Reference SOO Objective
Q-APP-4	Application growth – The goal is to create an environment where innovative and relevant applications are being produced for public safety users.	Continually increasing the total number of applications being published to the FirstNet applications store	Once a baseline* is met, 5% application quarterly growth for the first 3 years, 2% per quarter for the rest of the life of the contract * Baseline to be established at IOC-1	M3-MIS, M1-monthly	Total number of applications published to the FirstNet applications store that have at least 5% unique downloads by the target user group for the application. For example, 5% usage by registered fire users of a fire-focused application	Blue: Exceeds Acceptable Performance Level (APL) target by 1% (e.g., 6% instead of 5%) Green: APL rate plus up to 1% exceeding target Yellow: Between 0 and APL target Red: Declining number of applications	Sum of all applications in the FirstNet applications store that have at least 5% unique downloads by the target user group for the application	5

Table of Contents

1 Cybersecurity Objective

The cybersecurity solution implemented by the Contractor in connection with the contract with the First Responder Network Authority (FirstNet) must comply with the following provisions from the Middle Class Tax Relief and Job Creation Act of 2012 (the Act):

- Section 6206(b)(2)(A) requires FirstNet to "ensure the safety, security, and resiliency of the network, including requirements for protecting and monitoring the network to protect against cyberattack."
- Section 6206(c)(2)(A)(iv) requires FirstNet to "consult with regional, State, tribal, and local jurisdictions regarding the distribution and expenditure of any amounts required to [establish network policies] with regard to the adequacy of hardening, security, reliability, and resiliency requirements."
- Section 6203(c)(1)(A) required the Federal Communications Commission (FCC) to "develop recommended minimum technical requirements to ensure a nationwide level of interoperability for the nationwide public safety broadband network [NPSBN]." On June 21, 2012, the FCC approved by Order (FCC 12-68) the Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network (Section J, Attachment J-3, FCC TAB RMTR) that was released on May 22, 2012, *as clarified* on June 6, 2012.
- The Act also requires FirstNet to comply with the Third Generation Partnership Project (3GPP) (Section 6001); Long Term Evolution (LTE) (Section 6203); and open, non-proprietary, commercially available standards (Section 6206(b)(2)(B)(i)).

FirstNet refers to the overall cybersecurity approach as the NPSBN cybersecurity solution. The concepts contained in this document are critical to the successful development, implementation, evolution, and maintenance of the NPSBN cybersecurity solution. The solution will be a joint effort of FirstNet and stakeholders involved with the NPSBN.

2 NPSBN Cybersecurity Concepts

The NPSBN cybersecurity solution should be based on the following minimum cybersecurity concepts to ensure the NPSBN is protected, operating with an acceptable level of risk, and accessible for public safety users. These concepts should be considered critical to the design of the NPSBN cybersecurity solution.

2.1 Public Safety Needs

The NPSBN cybersecurity solution should ensure that the NPSBN is protected from cyberattack but also ensure public safety users can readily access the network. All critical operational equipment and functions, which could affect the secure and effective operations of the NPSBN, shall be located within the sole jurisdiction of the United States. To that end, the solution should take into account the following areas:

- **Usability** – The network should be usable by Public Safety Entities (PSEs). Security controls, policies, and procedures should provide protection without impacting operability or interoperability.

- **Mission Primacy** – The mission of public safety—to protect lives and property from clear and present danger—should take primacy over protection of the network.
- **Operational Security** – The NPSBN cybersecurity solution should protect public safety users from situations where a security breach leads to an operational security breach.
- **First Responder Safety** – The NPSBN cybersecurity solution should not negatively affect first responder safety or impair requests for assistance in a responder emergency or immediate peril situation.
- **Reliability/Resiliency** – The NPSBN cybersecurity solution should enhance the reliability and resiliency of the NPSBN.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA**) – Traffic and transactions governed by HIPAA and subsequent related laws will transit and potentially be acted upon within the NPSBN.
- **Criminal Justice Information Services (CJIS)** – Traffic and transactions governed by the Federal Bureau of Investigation's CJIS Security Policy will transit and potentially be acted upon within the NPSBN.
- **Payment Card Industry (PCI)** – Traffic and transactions requiring PCI compliance will transit the NPSBN.
- **End-to-End Encryption of User Communications and Data** – Public safety users expect their communications and data to be secure from end to end. Data loss prevention techniques should apply to all public safety data while at rest on the server/device, in transit, and in use. The NPSBN cybersecurity solution should encrypt user plane and signaling communications everywhere possible.
- **Privacy** – The privacy of the user and the user's data is as important as its cybersecurity and should be accounted for.
- **Authentication** – Authentication methodologies on the network and for devices should allow public safety easy access but provide a high level of security. The solution should include federated Identity, Credential, and Access Management (ICAM) in concert with appropriate multifactor and step-up authentication approaches.
- **Multi-Layer Security** – It is critical that the NPSBN support layered security policies that permit PSEs to implement their unique security policies, provided that doing so does not compromise the overall security of the NPSBN. Inherently, a PSE security implementation, layered on top of the NPSBN, will only be interoperable to users authorized by the jurisdictional security authority.
- **Data Protection** – The protection of public safety data is critical for PSEs and first responders. The solution should prevent unauthorized disclosure (confidentiality), modification (integrity), or the inability to access the data when it is needed (availability).

2.2 Dedicated Cybersecurity Program

The NPSBN cybersecurity solution should include a dedicated cybersecurity program that considers all source threats; constructs a dynamic threat profile; generates a cybersecurity architecture; builds in proactive forensics; and establishes incident response capabilities that ensure the ability to operate and deliver crucial services as needed during a national, state, or local incident.

2.3 Federal Requirements

The NPSBN cybersecurity solution should enable all relevant entities to meet applicable federal cybersecurity standards and requirements, including any applicable requirements under the Federal Information Security Modernization Act of 2014 (FISMA).

2.4 Cybersecurity Architecture

To establish a secure NPSBN, the network architecture should, at a minimum, implement the recommended requirements listed in Section 1.3.7, Security, and the recommended considerations listed in Section 1.4.8, Security, of Section J, Attachment J-3, FCC TAB RMTR, as well as the following 3GPP specifications: TS23.401, TS33.102, TS33.210, TS33.310, TS33.401, and TS33.402.

2.4.1 Industry Best Practices

The NPSBN cybersecurity solution should implement industry best practices for wireless carriers, information technology, and critical infrastructure, including but not limited to the following areas:

- **Transport Security** – The solution should protect the S1 interface (between the base station and Core) and all other communications planes between Evolved Node Base stations (eNodeBs) and Core sites, including S1, X2, and all other management and timing plane communications between these devices.
- **Domain Security** – The solution should protect the end-to-end network by dividing it into domains, providing protection between domains, providing security policies and procedures for each domain, and protecting any inter-domain traffic as well as traffic transiting domains. Domains may include the following:
    - Radio Access Network within a state or territory
    - Backhaul network (eNodeB to regional aggregation points)
    - Aggregation network (aggregation of traffic in a region)
    - National transport networks (network connections to regional and national Core sites)
    - Evolved Packet Core (EPC)
    - Business support systems
    - Operational support systems
    - Applications ecosystem
    - Internet Protocol (IP) Multimedia Subsystem
    - Value-added services
    - Messaging services
    - Public Safety Enterprise Network (PSEN) connectivity
    - FirstNet cloud environments
- **External Interface Protection** – The solution should safeguard all external interfaces with appropriate security protections, such as firewalls, protection from common Internet attack vectors (e.g., Denial of Service [DOS], Distributed DOS [DDOS], spoofing, malware, botnets, port scanning), intrusion prevention and detection, security gateways, security logging, and content inspection/filtering. External interfaces may include:
    - SGi interface
    - Roaming interfaces such as S8 and S6a
    - Public Switched Telephone Network (PSTN) and Voice over IP (VoIP) peering for voice and messaging traffic
    - PSEN interfaces
    - Network partner, network element provider, and other third-party remote connection interfaces required for on-call or emergency maintenance and troubleshooting
    - Applications ecosystem interfaces with content providers, application developers, and service providers offering services via the applications ecosystem

- **End-to-End Security Management and Logging** – The solution should support a security information and event management (SIEM) solution to enable security analysis of large volumes of collected data and enable interfaces to the NPSBN for information sharing purposes. Further details are contained in Section 2.12, Cybersecurity Network Management and Configuration Management Policy.
- **Fraud Prevention and Revenue Assurance** – The solution should include fraud prevention and revenue assurance functionalities to ensure that resources are being used appropriately and charging and service control transactions are providing a true picture of network usage.
- **Network Address Translation** – The solution should implement network address translation and other associated functions for end-user traffic. Where required, static addressing should be made available as well.
- **Protection Between Users** – Where appropriate, and not at the expense of operability, the solution should protect users from other users on the network. There are times when direct device-to-device communications through the network are required, such as user plane communication during an IP Multimedia Subsystem session, but attack vectors such as a ping of death, port scanning, and DOS should be prevented between end users.
- **Signaling Storms** – The solution should detect and prevent signaling storms both inside the network and on external signaling interfaces. This may be accomplished with Diameter Routing Agents and proxies.
- **Rogue or Stolen Devices** – The solution should protect against rogue devices and/or stolen devices (e.g., devices deemed an operability or security risk, devices that have been compromised, or devices that have not successfully passed device certification processes). The solution may include Equipment Identity Register functionality but should also include detection functionality. A device or class of devices should be able to be blacklisted/un-blacklisted either manually or automatically. Automatic blacklisting must not jeopardize the safety mission of first responders.
- **Heterogeneous Networks** – The solution should enable small cells and heterogeneous networks, potentially offered by a third party, to securely authenticate and interconnect to the Core network.
- **Operational Support System** – The solution should include an operational support system that implements FCAPS (fault management, configuration management, accounting management, performance management, and security management), authenticates all users connecting to network elements for maintenance and operations, and logs all access and configuration actions. Further details are contained in Section 2.12, Cybersecurity Network Management and Configuration Management Policy.
- **Domain Name Service (DNS) Security** – The solution should deploy a secure DNS solution and distinct DNS domains/zones for Transport Security, the evolved packet core, the roaming network, and the SGi interface. These domains/zones should be completely separate and distinct.
- **Messaging Security** – The solution should include a messaging security solution that protects the messaging infrastructure as well as the attack vectors within the messages themselves. This may include anti-virus, anti-spam, and malware protection as well as IP-reputation verification. Messaging may include email, instant messaging, short messaging, and multimedia messaging.
- **IP Multimedia Subsystem Security** – The solution should include an IP Multimedia Subsystem security solution that protects it from an infrastructure, signaling, and user-plane prospective.
- **Business Support Systems Security** – The business support systems should include but not be limited to mediation, charging, billing, provisioning, local control, and customer relationship

management. These systems should be protected and include access control and full transactional logging.

- **Mobile Virtual Private Networks (mVPNs)** – The solution should enable an mVPN solution to ensure PSEs can securely communicate and still utilize Quality of Service, Priority, and Preemption. If secure communications are required by public safety for network services such as messaging, NPSBN cloud services, or IP Multimedia Subsystem, then mVPNs should be able to be terminated inside the Core network.
- **Business Continuity Planning, Disaster Recovery Planning, and Crisis Management** – The solution should utilize industry best practices for business continuity planning, disaster recovery planning, and crisis management.
- **IP Infrastructure Network Elements** – The solution should ensure all routing and switching network elements are hardened and configured to only allow traffic that is required to transit the network using access control lists and other methodologies.
- **Security Hardening** – All network elements should be hardened according to defined policy, process, and guidelines and should be continuously monitored for compliance. Specifically, security hardening should include:
    - Patch maintenance
    - A security hardening tool portfolio
    - Access control, including the associated system configuration and policy
    - File system hardening and access control
    - Network security
    - Process security
    - Host logging
    - Time synchronization
- **Cybersecurity Governance Model** – The cybersecurity governance model should include a security governance organization; security governance policies; security functional requirements; security risk identification, analysis, and mitigation; security technical controls; security operational controls and procedures; security responsibilities and practices; strategies and objectives for security; risk assessment and management; and resource management for security.
- **Supply Chain Cybersecurity** – The solution should ensure the cybersecurity of the supply chain throughout the life of the contract is verifiable and that no vulnerabilities, exploits, or threat vectors have been introduced to products prior to installation in the NPSBN.
- **Training** – Human factors within cybersecurity are considered as one of the most important but most difficult areas to assess and protect. The solution should provide training for users and operators to increase the cybersecurity of the NPSBN.
- **Insider Threat Mitigation** – The NPSBN cybersecurity solution should include prevention, control, mitigation, and detection of insider threats.
- **Cloud Security** – There should be a robust cybersecurity solution for any cloud services offered within the NPSBN. The cloud security solution should provide identity management tied to that of the NPSBN, physical security, personnel security, availability, application security, and privacy.
- **Virtualization Security** – As virtualization becomes more common, even within the EPC through Telco Cloud and network-functions virtualization, the cybersecurity of the virtual environment requires additional focus to ensure there are no cyber risks introduced to the network through virtualization.
- **VoIP Spam** – The solution should mitigate VoIP spam, or Spam over Internet Telephony, as well as “robodialing.”

2.4.2 Devices and Applications

To ensure the security of User Equipment (UE) and devices, the NPSBN cybersecurity solution should include but is not limited to the following elements:

- **Secure Operating System Architecture**
  - Boot loaders, which initiate the operating system (OS) of the device, should not be allowed to be tampered with by malware. OS vendors now take on the responsibility of building bootloaders into their software instead of employing third-party software.
  - [bullet removed]
  - The secured container solution should be used to protect agency applications and user data in mobile devices. Security policy guidelines and processes should be used for secured container solution in protecting agency data with a user's personal application.
  - Devices should be continuously monitored both online and offline to ensure the OS is not compromised and that devices have not been "jail broken" or "rooted."
  - FirstNet and its selected Contractor will work with device manufacturers on OS updates related to security issues and local control Mobile Device Management (MDM) solutions to enable PSEs to provide updates to public safety users.
  - The device local storage must be encrypted with OS capability.
- **Authentication of Users and Applications**
  - MDM should enable the PSE administrator to enforce device and application password policies remotely.
  - MDM should enable authentication for access to the collection of secured applications on the device.
  - Certificate or token-based authentication of certified applications should be available.
  - Device-specific biometric authentication (e.g., fingerprint, retina) should be integrated for supplemental authentication of certified access to the application.
- **Embedded Applications**
  - Latency-sensitive mission-critical applications (such as Mission-Critical Push-to-Talk) should be signed and certified (validated as prescribed by FirstNet) and should be provided to various Original Equipment Manufacturers as part of pre-installed applications on the device.
  - Internal embedded clients should use non-exposed Access Point Names (APNs) for access all certified applications or for PSE network access.
- **MDM and Mobile Application Management (MAM) – PSE-Managed Whitelist/Blacklist**
  - The PSE administrator should be able to wipe or lock a lost or stolen device.
  - The PSE administrator should be able to manage applications on devices through MDM.
- **Digital Signature of the Applications** – Digital signatures of FirstNet and partners' signed applications should be verified by the device.
- **Device Security Solutions** – Device security solutions should be provided, including smartphone/device security that includes anti-virus; firewall; remote management of applications and services; monitoring; theft prevention; device access control; and protection of the UE by the network with content inspection/filtering, messaging security, and the protections provided through other methodologies in this section.
- **Bring Your Own Stuff** – Cybersecurity solutions should address Bring Your Own (Device, Application, or Wearable) approaches.

2.4.3 Application Security

To ensure the security of applications, the NPSBN cybersecurity solution should include but is not limited to the following elements:

- **Applications Ecosystem Security** – The solution should provide protection for the NPSBN applications ecosystem, including the associated applications store, application development environment, cloud services, Service Delivery Platform (SDP), Application Programming Interface (API), applications, and the PSE networks. The Offeror-provided public safety applications and data, local control, and agency home page portal need to be secured and protected against all threats, including external threats, internal threats, data breaches, and DOS attacks.
- **API Security** – The Contractor will develop new NPSBN capabilities and services and expose specific APIs to enable new applications. These APIs, services, and applications will allow for new capabilities such as dynamic control of Quality of Service, priority, preemption, local control, agency home page status, and public safety analytics. APIs give developers—both legitimate developers and potential system hackers—more finely grained access into an application than a typical Web application. The solution should address API threats, including but not limited to the following:
    - Parameter attacks that exploit the data sent into an API, including URL, query parameters, HTTP headers, and/or posted content
    - Identity attacks that exploit authentication, authorization, and session tracking
    - Man-in-the-middle attacks that intercept legitimate transactions and exploit unsigned and/or unencrypted data
    - Protection of sensitive APIs from unauthorized use
- **Application Audit** – Proper logging and auditing can provide invaluable information and uncover more than just security concerns. The solution should ensure applications properly log and audit the actions by the user and information about the user who takes those actions.
- **Application Security in Software Development Life-Cycle** – The solution should promote secure programming and provide developers with tools to ensure they keep security in mind throughout the software development process. Currently, there are several code analysis and test tools available commercially or through open source.
- **Application Security Certification** – The solution should ensure the NPSBN's application security and certification process includes analyzing the application both statically and dynamically for security vulnerabilities. Making these tools and methods available to developers in order to catch vulnerabilities and potential risks as early as possible in the development life-cycle is critical. Such tools and assessments should be continually used, even after an application has been certified, because the security landscape changes with new risks and vulnerabilities discovered daily. The solution should ensure all mobile, Web, and desktop applications published on the NPSBN applications store (also referred to as the "FirstNet applications store") undergo a defined certification process to ensure usability, reliability, privacy, security, and safety. This process should allow PSEs to have a high degree of confidence when downloading or purchasing certified applications from the NPSBN applications store.
- **Application Developer Certification** – The application developers registering with the NPSBN and publishing the applications should be audited and certified apart from the applications.
- **User Logging** – The solution should ensure administrators and users accessing the application ecosystem are logged audited and transactions are recorded. Proper logging and auditing can provide invaluable information and uncover more than just security concerns.

- **End-to-End Application Analysis** – The solution should leverage a log analysis tool to analyze application, Core, network, and other log files. There are several advanced tools available that allow for real-time analysis and generate alerts based on events detected by analyzing log files and other information feeds. These can provide the Security Operations Center with detailed views into the behavior of the applications ecosystem and provide vital security reports and information.
- **Validation of Application-Specific Port Monitoring** – Any non-standard ports used by an application need to be monitored for any security breach.
- **Application Protection** – The solution should provide protections to ensure only approved applications are loaded and run on a UE.
- **Application-Device Security** – The solution should provide protections to ensure applications cannot bypass OS security on devices.
- **Data Loss Prevention** – The solution should provide protections to ensure applications protect data while at rest, in use, and in transit.
- **Secure Application Coexistence** – The solution should provide a secure method of coexistence among NPSBN-certified applications and commercially available applications on a device.

2.4.4 Strong Identity, Credential, and Access Management

To ensure the security of user identities, the NPSBN cybersecurity solution should include but is not limited to the following elements:

- **ICAM** – The solution should support federated identity from PSE networks.
- **Identity Assurance** – The solution should ensure the following relationships are authenticated:
    - User to Device – PSEs may not acquire one device for every user. It therefore becomes critical to know which first responder has the device.
    - Device to Network – LTE authentication
    - Network to Application – Identity management
    - Network to PSE Network – Identity management
    - User to Application – Identity management
    - User to PSE Network – Identity management
- **Authorization** – The solution should ensure users are properly authorized to access applications, data, and services through the use of Attribute Based Access Controls (ABAC), Policy-Based Access Controls (PBAC), and similar methods.
- **Credentialing** – The solution should ensure that agencies are following the process for identity proofing users and assigning credentials.
- **Auditing** – The solution should ensure that all user actions are properly monitored and audited.

2.4.5 Cryptography

LTE is designed with strong cryptographic techniques, mutual authentication between LTE network elements, and security mechanisms built into its architecture. With the emergence of the open, all IP-based, distributed architecture of LTE, attackers can target mobile devices and networks with spam, eavesdropping, malware, IP-spoofing, data and service theft, DDOS attacks, and numerous other variants of cyberattacks and crimes. This will necessitate appropriate safeguards and mitigation approaches to negate the impact of these attack vectors.

2.4.6 Public Safety Enterprise Network Security

The NPSBN cybersecurity solution should recommend minimum security standards for state and local agencies. The solution should include initiatives to educate state and local agencies on cybersecurity topics related to the NPSBN and to review and advise agencies on strengthening their security architectures and policies, if needed, prior to connecting to the NPSBN.

2.5 Cybersecurity Life-Cycle Process

The NPSBN cybersecurity solution should include an ongoing cybersecurity life-cycle process that employs and monitors security controls, ensuring continued viability and effectiveness of the NPSBN. The primary areas of this process include the following, which are performed in a recurring cycle over time as older threats and vulnerabilities become negated and new ones arise:

- Identifying vulnerabilities
- Identifying threats
- Determining risks arising from threats and vulnerabilities
- Prioritizing risks to determine associated controls
- Specifying controls to address or mitigate threats and vulnerabilities
- Implementing controls
- Assessing the effectiveness of controls
- Monitoring the security of the system

Key to this ongoing approach will be 3GPP feature enhancements and major release upgrades being made available and implemented on the NPSBN. The solution should include a plan to address associated support for security upgrades to network infrastructure and devices as capabilities advance generationally. The solution should include provisions to establish security support for aging network infrastructure and devices and sunset procedures for network infrastructure and devices when they are no longer viable.

2.5.1 Identifying Vulnerabilities

Vulnerabilities can surface in virtually all aspects of the NPSBN enterprise. It is critical to be aware and capable of identifying those vulnerabilities present in software (e.g., OSs, applications, protocols, encryption), hardware, firmware, and related capabilities. Vulnerabilities will need to be documented appropriately to permit development of suitable controls as well as determine the effectiveness of those controls.

2.5.2 Identifying Threats

Threats can take multiple forms and provide attack vectors to all components of the NPSBN enterprise. The Core network, Radio Access Network, UE, applications, and backhaul transport are subject to a range of threats. The threats will need to be documented appropriately to permit the development of suitable controls as well as determine the effectiveness of those controls.

2.5.3 Determining Risks Arising from Threats and Vulnerabilities

Once the relevant threats and vulnerabilities have been identified and documented, it will be necessary to determine the risks tied to each. In some cases, the risk will be sufficiently improbable as to not require any action. For all others, an impact determination will be accomplished to rank where the risk falls relative to other risks.

2.5.4 Prioritizing Risks to Determine Associated Controls

After risks have been assigned respective impact determinations, they will be ranked in order of criticality to determine mitigation. Risks that have no direct correlation to an internally controlled mechanism will be either accepted or transferred (e.g., through procurement of insurance against the risk). Those risks tied to a particular vulnerability or threat will be evaluated based on impact and viability of mitigation. Upon final ranking and evaluation, appropriate controls will be addressed.

2.5.5 Specifying Controls to Address or Mitigate Threats and Vulnerabilities

Once the threats and vulnerabilities have been identified and prioritized, suitable controls will be identified to mitigate them. In the event, there is no viable control to address a threat or vulnerability, a determination of acceptance of risk and a proposed fix should be documented and provided. Revalidation should occur periodically, but no less than quarterly, to determine if the proposed fix is available and if the current acceptance is still sufficient.

2.5.6 Implementing Controls

All selected and specified controls will be implemented prior to Initial Operational Capability when possible; those controls developed subsequently or as new controls supersede existing solutions will be implemented as quickly as possible but not before ensuring they do not introduce unanticipated problems elsewhere. Implementation of controls will adhere to the guidance found in Section 2.12, Cybersecurity Network Management and Configuration Management Policy.

2.5.7 Assessing the Effectiveness of Controls

After implementation, the effectiveness of the specified controls will be assessed on an ongoing basis to ensure they perform their function as expected. The results of the ongoing assessment will be documented appropriately and retained for situational awareness.

2.5.8 Monitoring the Security of the System

The NPSBN will be monitored for performance and security and security control indicators will be tracked to determine their effectiveness against identified threats. Monitoring will also be used to develop awareness of new threats and begin the cybersecurity life-cycle process again, if needed. The process is iterative and does not end as new threats and the need for associated security controls continues indefinitely.

2.6 Cybersecurity Guidance

There is considerable cybersecurity guidance available from industry, government, and standards organizations that should be considered when developing the NPSBN cybersecurity solution. There is no single solution or guidance that addresses all cybersecurity challenges. When considering the complexity of the NPSBN and the fact that its components, users, and usage falls into many different cybersecurity areas of practice, the NPSBN cybersecurity solution should employ multiple frameworks to address these needs.

2.7 Cybersecurity Systems Engineering

The NPSBN cybersecurity solution should take into account the best practices of systems engineering but expand them with the best practices of cybersecurity engineering. Cybersecurity systems engineering should:

- Include a cybersecurity systems engineering plan that enumerates operational policies and procedures at all levels.
- Include a repeatable process that is executed continuously both during the development and evolution of the NPSBN.
- Ensure cybersecurity engineering is considered in all decisions, designs, and actions related to the NPSBN. The network should meet the core tenets of cybersecurity for a modern, robust wireless communications system while following the principles of systems engineering, including documented and robust use of the people, processes, and technology required to provide security with minimal impact to the user population.
- Maintain the simple, overarching cybersecurity principles of the NPSBN:
    - Ensure the network is being used by only the authorized personnel it supports
    - Ensure the network and its users are protected from all others, whether they are external adversaries or insider threats
    - Ensure the cybersecurity program is robust and capable of detecting if any of the cybersecurity principles are not true
- Ensure the cybersecurity design of the network and components:
    - Plans, develops, and tests new technologies
    - Performs technical analysis in support of development and test activities for new systems and emerging technologies
    - Facilitates the development of future requirements and architecture components to enable the transition of new systems and technologies into the operational baseline
    - Coordinates future technology efforts with internal and external partners and operational users
- Facilitate cybersecurity assessment, including but not limited to:
    - Utilizing a third-party, independent organization to provide laboratory and field security assessments
    - Performing independent verification of NPSBN planning and infrastructure
    - Adopting best practices from other federal agencies and industry
    - Running large-scale scheduled cybersecurity exercises and targeted local cybersecurity exercises as needed
- Utilize resilient design principles, including but not limited to:
    - Engineering a resilient network. This requires balancing single points of failure and economics
    - Aligning with 3GPP Release 9 LTE, which introduces IP as the basic connectivity between network elements.
    - Securing the NPSBN's network architecture, which will ensure that single points of failure are reduced as low as economically reasonable. The impact of single points of failure can be reduced by utilizing:
        - Self-Organizing Networks
        - Site hardening (physical security)

  - Layers of network coverage
  - Industry best practices to protect against systemic failures, cyberattacks, and human errors
- Establish application security policies and procedures that encompass distribution of applications that can be used on the NPSBN.

2.8 Cybersecurity Risk Management

The NPSBN cybersecurity solution should have a detailed and robust risk management methodology that is executed continuously during the system's development life-cycle and during the life of the program and the NPSBN.

The risk management methodology should, at a minimum, contain the following steps:

- Asset identification
- Risk impact analysis
- Threat assessment
- Risk mitigation
- Security control selection and deployment
- Risk mitigation operations and maintenance

The methodology could be based on or enhanced by existing models, such as the National Institute of Standards and Technology (NIST) Risk Management Framework or the ISO 27000 series.

2.9 Cybersecurity Incident Response and Security Operations Center

The NPSBN cybersecurity solution should address incident reporting and response, which are critical to the security of the NPSBN. If an incident or event is deemed to require travel to a site for additional security investigation and analysis, the Government will require the Contractor to dispatch staff within a time period to be established, but potentially in as little time as one business day.

2.9.1 Cybersecurity Incident Response Team

The NPSBN cybersecurity solution should account for a Cybersecurity Incident Response Team that will be responsible for managing incident response. At a minimum, the team should perform the following activities:

- Coordinate the notification and distribution of an incident
- Mitigate the risk of an incident by minimizing disruptions
- Notify the contracting officer if it appears that the mitigation will have an associated cost
- Assemble security staff to conduct a threat assessment and resolve the incident
- Take reasonable steps to mitigate the effects and to minimize any damage resulting from the incident
- Monitor system logs for application to the incident
- Categorize all security incidents per policies and procedures and report them within specific time frames, to be identified
- Define and capture metrics that will be used for reporting

- Provide a post-mortem for each incident associated with an actual cyberattack in a format agreed upon by the Contractor and FirstNet
- Provide an after action report for any incident that occurs due to inadvertent actions by authorized operations and maintenance personnel in a format agreed upon by the Contractor and FirstNet
- Record or log all security incidents in an electronic format (to be determined). These logs will provide the information for reporting purposes
- Report all security incidents based on incident severity, as directed in standard operating procedures that will be developed jointly between the Contractor and FirstNet

All incidents must be immediately reported, whether suspected or confirmed, including potential risks to the confidentiality, integrity, or availability of NPSBN information or to the function of NPSBN systems.

Upon becoming aware of any unlawful access to data or information stored on the Contractor's equipment or in the Contractor's facilities, or unauthorized access to such facilities or equipment resulting in the loss, disclosure, or alteration of any FirstNet data or information (a "Security Incident"), the Contractor should notify the Contracting Officer immediately.

2.9.2 Security Operations Center

The NPSBN cybersecurity solution should include a Security Operations Center that provides:

- Situational awareness, including collecting, maintaining, and sharing information about threats to network infrastructure, devices, data, and applications
- 24/7/365 cybersecurity monitoring of Core network infrastructure, devices, data, and applications
- Monitoring and analysis of user, system, and network access
- Assessment of the integrity of the system and data files
- Establishment of the baseline network activity and utilization to use as a reference
- Recognition and analysis of activity patterns that are indicative of an incident or intrusion
- Analysis of logs for abnormal use patterns
- Information sharing and collaboration that integrates and disseminates information throughout the critical infrastructure partnership network
- Processing and posting suspicious activity reports
- Assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications
- Decision support that provides recommendations to partners and FirstNet leadership

2.10 Cybersecurity Continuous Monitoring and Mitigation Methodology

The NPSBN cybersecurity solution should include a cybersecurity continuous monitoring approach and mitigation methodology that addresses the following elements:

- Continuous Monitoring and Forensics – The solution should adopt active security tools and solutions that continuously monitor, log, and provide forensic data about the current state of the network and any changes that have occurred.

- The solution should support a continuous monitoring approach that includes the following components and processes:
    - Hardware Asset Management – the automated means of tracking which components are on the network and their associated attributes. This ensures awareness of what systems are operating and that they are legitimate components.
    - Software Asset Management – the automated means of tracking software running on the network and ensuring consistent versions and releases are the only ones permitted to run and those failing the mark are upgraded or removed.
    - Vulnerability Management – entails scanning software throughout the network as well as traffic traversing the network for signatures or behavior that are atypical. Items identified in vulnerability scans are then referred for analysis and further investigation.
    - Configuration Settings Management – deals with settings on network components, such as router access control lists or firewall settings. An automated toolset evaluates settings against baseline standards to ensure consistency of configuration as well as ensuring simple typos do not result in compromising the network.
- Mitigation of identified issues from continuous monitoring takes multiple forms and is dependent on the nature of the specific issue. For example, determining if misconfigured hardware is updated with the correct settings requires different mitigation solutions than ensuring out-of-date software is patched and/or replaced.

2.11 Cybersecurity Testing and Certification Plan

The NPSBN cybersecurity solution should include a testing and certification plan that is tailored to cybersecurity issues. The plan should, at a minimum, address the following areas:

- **Testing Life-cycle** – Processes should be established to verify security approaches through a life-cycle of selection, procurement, integration, and operations support. This is often a key functionality within an organization's greater cybersecurity systems engineering practice. The testing methods will include assessment, testing, examination, and interviewing. All testing results should be retained to provide baseline standards for ongoing testing to ensure optimal accuracy and reproducibility.
    - Assessment is the process whereby a security control is evaluated as to how well it meets stated security objectives.
    - Testing is the subjection of the security control to inputs to determine what results occur.
    - Examination is the review of related documentation for one or more controls to determine stated objectives and capabilities.
    - Interviewing is the discussion with designers, implementers, and users regarding the expectations and behaviors of the stated controls on the system.
- **Individual System Validation** – Individual systems should be validated by an independent assessor in a continuous improvement and feedback fashion to maximize the depth and value of the assessment, as well as to test the responsiveness to the process.
- **Integrated Configuration Testing** – Pilots for user functionality enable successful full-scale security scanning, assessment, and testing for new vulnerabilities introduced as part of the fielding process, as well as testing of initial security monitoring, intrusion detection, and cyber incident response capabilities.

- **Independent Applications/Services Testing** – All applications that are distributed by the Core network or exchange data with the Core network should undergo formal testing, validation, and authentication prior to distribution to provide reasonable assurance of their respective security posture. For evolving integration with PSE networks, the security policies and posture can be determined by application data flows (local vs. national) and the use of distinct gateways that can defend those boundaries. Testing and validation should address applications for each of the following situations, as appropriate in the life-cycle of the application as well as its origination:
    - New applications at the national level
    - User-developed or state-developed applications
    - Upgrades to currently approved applications
    - Security patches to currently approved and fielded applications

2.12 Cybersecurity Network Management and Configuration Management Policy

The NPSBN cybersecurity solution should include policies for network management and configuration management.

2.12.1 Network Management

The NPSBN cybersecurity solution should involve the management and maintenance of cybersecurity tools and capabilities by an out-of-band network that limits access to devices to a small number of authorized personnel. If this is not practical, then alternative methods, such as a Virtual Private Network (VPN), should be employed.

2.12.2 Configuration Management

In the context of cybersecurity, configuration management is the practice of handling changes to security tools, software, and devices in a repeatable, systemic manner to ensure the security and the integrity of the security processes over time. Configuration management will be developed and implemented to ensure cohesive policies, procedures, techniques, and tools to manage, evaluate a proposed change, track the status of implementation of any approved changes, and maintain the artifacts of system and support documents as they change. From the American National Standards Institute/Electronic Industries Alliance standard 649, the five distinct disciplines should be:

- Configuration Management Planning and Management
- Configuration Identification
- Configuration Control
- Configuration Status and Accounting
- Configuration Verification and Audit

2.12.3 Vulnerability Management

The NPSBN cybersecurity solution should include a methodology to conduct and maintain routine, consistent vulnerability scanning of NPSBN infrastructure that is passive in nature to ensure no impact to systems. Any discovered vulnerabilities should result in efficient, effective remediation.

2.12.4 Patch Management

The NPSBN cybersecurity solution should establish a continuous cycle of applying software updates and patches for all software provided with the system, including OSs and third-party applications. Patches

should be thoroughly vetted through a verification and validation lab. This will provide NPSBN users and leadership assurance that the patch updates will not negatively impact the operational capabilities of the wireless communications system. A critical aspect of a patch management solution for wireless communications systems is the ability to test critical vulnerabilities out of cycle, which cannot wait until the next scheduled patch distribution.

The solution should adhere to industry best practices for a patch management solution, including:

- Centralized, role-based administration
- Integration with an authentication and authorization server
- Patch scheduling and administration
- Air-gap patches capability, which requires updating the patch management server with mobile media (e.g., DVD or thumb drive) without connectivity to the Internet required

2.12.5 Centralized Security Log Management

The NPSBN cybersecurity solution should include SIEM—a tool focused on the security aspects of log management, which involves collecting, monitoring, and analyzing security-related data from computer logs. Security-related data includes log data generated from numerous sources, including antivirus software, intrusion detection systems, file systems, firewalls, routers and switches, and servers. SIEM is responsible for the aggregation and normalization of security-related data and allows for analysis on a large number of logs in an efficient manner.

2.13 Environmental and Physical Security

Environmental and physical security is critical to security planning for any information systems. This capability is one of the most mature tenets of security. However, because the NPSBN will be disparately deployed across the nation, environmental and physical security can quickly become cost-prohibitive. Environmental and physical security systems should be capable of monitoring alarms, centrally displaying and reporting the alarm status of the entire system and all sub-components, and forwarding critical alarm notifications to appropriate personnel within the Network Operations Center or Security Operations Center.

The NPSBN cybersecurity solution should take into consideration the following physical and environmental security elements:

- Power Failure
- Humidity Detection
- Cabinet Door Alarms
- Uninterruptable Power Supply Power Failure
- Access Control to and Within a Facility
- Monitoring and Recording of Activity Within a Facility to Include Egress/Ingress
- Movement Activity Within a Facility After Hours or in Restricted Areas
- Heating, Ventilation, and Air Conditioning (HVAC) Failure or Degradation
- Building Door Alarms
- Generator Failure
- Low Generator Fuel
- Low Battery
- Closed Circuit Television (CCTV) Video Surveillance Systems

- Fire/Smoke Detection Sensors
- Protection from Natural Disasters (e.g., lightning/surge protection, water leak detection)

2.14 Information Security and Data Sensitivity

All data in transit, accessed, or stored across the NPSBN environment will be encrypted and handled as restricted data. The use, dissemination of, and access to restricted data are limited to specific agencies, individuals, and situations. Where existing data repositories employed by NPSBN users already have established levels of mandated sensitivity and protection, those levels should be used at a minimum. Retention of any data will be in accordance with agency record retention policy as specified by the respective data owner. Upon expiration of the retention period, data should be destroyed or otherwise disposed per agency policy. Data in the NPSBN should not be releasable to any external parties without compliance with applicable laws.

Table of Contents

List of Tables

Executive Summary

<All instructional text is in Italic green font color and contained within the symbols "<" and ">". These should be deleted prior to document submission.>

<The purpose of this template, upon completion, is to describe, at a high level, the Offeror's overall test strategy. The Offeror shall use the Section J, Attachment J-8, IOC/FOC Target Timeline; Section C, Statement of Objectives (SOO); and the Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network (herein referred to as the FCC TAB) as references when completing this template. Section J, Attachment J-8, IOC/FOC Target Timeline, describes at a high level what features and functions need to be delivered by the Offeror and when they need to be delivered.>

<The Offeror shall add a brief Executive Summary.>

<The Offeror shall include key information in this document, including but not limited to the following:

- *A mapping of SOO and FCC TAB items to Initial Operational Capability (IOC) and/or Final Operational Capability (FOC) milestones*
- *A description of the strategy employed to verify the SOO and FCC TAB*
- *A high-level description of what test configurations and types of test environments will be employed per IOC and FOC*
- *A high-level description of the entrance and exit criteria per IOC and for the FOC*
- *A section describing the test strategy schedule and test management*
- *A section describing the necessary equipment, test tools, and training>*

1 Introduction

<The Offeror shall add a brief, high-level introduction describing the overall test strategy scope that will be employed to validate the FCC TAB and SOO per IOC and for the FOC.>

2 Test Strategy

2.1 Test Approach

<Using Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones below, the Offeror shall briefly describe the test approach that focuses on the end-to-end system level testing that will be completed at each major milestone of the NPSBN rollout. The milestones planned for the NPSBN can be found in Section J, Attachment J-8, IOC/FOC Target Timeline. This IOC/FOC schedule maps system functionality to each IOC/FOC milestone. End-to-end testing is planned at milestones IOC-1 through IOC-5 and FOC.>

<In addition to Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones below, the Offeror will describe their test strategy for the following items in the sections following the table:

- *User Equipment (UE) Test Strategy*
- *Radio Access Network (RAN) Test Strategy*
- *Evolved Packet System (EPS) and IP Multimedia Subsystem Test Strategy*
- *Network Services/Service Delivery Platform Test Strategy*
- *Application Test Strategy*
- *Operational Support System (OSS) and Business Support System (BSS) Test Strategy*
- *End-to-End Regression Test Strategy>*

Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
C.5-1: BUILDING, DEPLOYMENT, OPERATION, AND MAINTAINENANCE OF THE NPSBN	Refer to Section C.5-1 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-2: FINANCIAL SUSTAINABILITY	Refer to Section C.5-2 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-3: FIRST RESPONDER USER ADOPTION	Refer to Section C.5-3 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-4: DEVICE ECOSYSTEM	Refer to Section C.5-4 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-5: APPLICATIONS ECOSYSTEM	Refer to Section C.5-5 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-6: ACCELERATED SPEED TO MARKET	Refer to Section C.5-6 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-7: USER SERVICE AVAILABILITY	Refer to Section C.5-7 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-8: SERVICE CAPACITY	Refer to Section C.5-8 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-9: CYBERSECURITY	Refer to Section C.5-9 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-10: PRIORITY SERVICES	Refer to Section C.5-10 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
C.5-11: INTEGRATION OF STATE-DEPLOYED RANs	Refer to Section C.5-11 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-12: INTEGRATION OF EXISTING COMMERCIAL/FEDERAL/STATE/ TRIBAL/LOCAL INFRASTRUCTURE TO SUPPORT NPSBN SERVICES	Refer to Section C.5-12 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-13: LIFE-CYCLE INNOVATION	Refer to Section C.5-13 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-14: PROGRAM AND BUSINESS MANAGEMENT	Refer to Section C.5-14 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-15: CUSTOMER CARE AND MARKETING	Refer to Section C.5-15 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
C.5-16: FACILITATION OF FIRSTNET'S COMPLIANCE WITH THE ACT AND OTHER LAWS	Refer to Section C.5-16 of the SOO	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-01-F	Hardware and software systems comprising the NPSBN shall implement interfaces consistent with Table 2: Standards Implementation Methodology.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-02-F	Hardware and software systems comprising the NPSBN shall support the interfaces enumerated in Table 1: Minimum Interoperable Interfaces.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-03-F	Hardware and software systems comprising the NPSBN shall support management functions.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-04-F	Hardware and software systems comprising the NPSBN shall support Access Point Names (APNs) defined for PSAN usage.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-05-F	Hardware and software systems comprising the NPSBN shall support nationwide APNs for interoperability.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-06-F	Hardware and software systems comprising the NPSBN shall enable Quality of Service (QoS) control for PSAN-hosted applications via the 3rd Generation Partnership Project (3GPP) _Rx' interface.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-07-F	The NPSBN shall support IPv4, IPv6, and IPv4/v6 Packet Data Network (PDN) types defined in 3GPP TS 23.401.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-08-F	The NPSBN shall support IPv4 and/or IPv6 transport for the Evolved Packet System (EPS) interfaces enumerated in Table 1: Minimum Interoperable Interfaces, consistent with the FirstNet design.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-09-F	Any sharing agreement that FirstNet enters into shall implement network sharing according to 3GPP TS 23.251 and shall not impact public safety operations.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-10-F	The NPSBN shall include the capability to collect and convey UE location data to applications using a standardized interface in nearly real time.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-11-F	The NPSBN shall be capable of providing public safety subscribers with access to the global Internet.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-12-F	All UEs deployed on the NPSBN shall conform to the 3GPP Release 9 Uu interface enumerated in Table 1: Minimum Interoperable Interfaces.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-13-F	All UEs deployed on the NPSBN shall conform to the 3GPP TS 36.306 UE Radio Access Capabilities, Release 9.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-14-F	All UEs shall support interworking of the device with the USIM/USAT applications on the Universal Integrated Circuit Card (UICC) in accordance with the relevant 3GPP 31.101, 31.102, and 31.111 standards.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-15-F	All UEs deployed on the NPSBN that support roaming onto commercial Long Term Evolution (LTE) networks shall operate on any FirstNet roaming partner network using bands supported by the device.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-16-F	All UEs shall support dual IPv4/IPv6 stacks.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-17-F	Prior to IOT and system-level testing, UEs shall have met 3GPP conformance and certification requirements per an independent conformance testing organization (e.g., PCS Type Certification Review Board).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-18-F	Prior to operational deployment on the NPSBN, UEs shall have passed FirstNet-required interoperability testing (e.g., using a subset of applicable test cases from CTIA IOT and UICC functional test cases, vendor IOT, or similar commercial LTE industry practice).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-19-F	Prior to operational deployment on the NPSBN, UEs shall have passed FirstNet-required UICC functional testing.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-20-F	Prior to operational deployment on the NPSBN, infrastructure equipment shall have passed FirstNet-required interface conformance testing (e.g., testing S1-MME [Mobility Management Entity] conformance to 3GPP) on the interfaces specified by FirstNet.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-21-F	Prior to operational deployment on the NPSBN, infrastructure equipment shall have passed FirstNet-required interoperability testing at a system level as per the specific IOT requirements for the NPSBN.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-22-F	Infrastructure deployed on the NPSBN shall be included in the FirstNet-required First Office Application (FOA) process as part of the NPSBN deployment.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-23-F	The equipment comprising the NPSBN shall provide backwards compatibility of interfaces, from time of deprecation, for a minimum of two full major release/upgrades of the network. This requirement may be waived (i.e., interface obsolescence accelerated) if FirstNet can ascertain from the user community that there are no dependencies on a given interface.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-24-F	The NPSBN shall support user mobility across the entire NPSBN (including state-deployed RANs).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-25-F	The NPSBN shall support S1 and shall preferentially support X2 handover between adjacent NPSBN cells (including cells owned by states that assume responsibility for deploying their own RAN) whose proximity supports a handover opportunity.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-26-F	If roaming between the NPSBN and commercial LTE networks is implemented, the NPSBN shall follow GSMA PRD IR.88.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-27-F	If roaming between the NPSBN and commercial 3GPP 2G/3G networks is implemented, the NPSBN shall follow 3GPP TS 23.002 to support roaming into 3GPP 2G/3G networks.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-28-F	If roaming between the NPSBN and commercial 3GPP2 (eHRPD) networks is implemented, the NPSBN shall follow 3GPP 23.402 to support roaming into 3GPP2 (eHRPD) networks.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-29-F	The NPSBN shall support the use of mobile VPN technology to support mobility between the NPSBN and other networks.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-30-F	The NPSBN shall provide the ability for national, regional, and local applications to dynamically change a UE‘s prioritization and QoS using the 3GPP _Rx‘ interface.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-31-F	The NPSBN shall support all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-32-F	QoS mechanisms in the NPSBN shall comply with 3GPP TS 23.203.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-33-F	The NPSBN shall support the usage of all 15 ARP values defined in 3GPP 23.203.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-34-F	The NPSBN shall support the ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-35-F	The NPSBN shall implement a nationwide scheme for assigning access classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-36-F	The NPSBN shall implement a nationwide scheme for assigning QoS class identifier priority to IP network and backhaul priority across the entire NPSBN.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-37-F	The NPSBN shall support the use of industry standard VPN and MVPN technology, while providing priority and Quality of Service for encapsulated applications.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-38-F	The NPSBN shall use a nationwide common security profile for user plane and control plane traffic between UEs, eNBs and MMEs, in accordance with 3GPP LTE Network Access Domain protocols. The profile shall be based on 3GPP TS 33.401, and will be determined by FirstNet based on a system design and other considerations as it deals with evolving cyber threats. As a minimum, the profile shall include specification of ciphering algorithms (for example, use of AES-128 vs. SNOW 3G).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-39-F	The nationwide common security profile shall include ciphering of control plane traffic in order to provide for interoperable cyber protection of the network. Ciphering of user plane traffic is optional and is based on policy decisions that involve FirstNet and user agencies.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-40-F	To enable interoperable authentication, the USIM and HSS shall be capable of supporting the same key derivation functions, such as Milenage per 3GPP TS 35.205, 35.206.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-41-F	Network domain security shall be implemented in accordance with 3GPP TS 33.210, which stipulates the use of IPSec to protect IP communication between administrative domains (including all network connections used to interconnect the domains).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-42-F	The NPSBN shall comply with TS 33.310 as the authentication framework for Public Key Infrastructure to authenticate these network interfaces.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-43-F	In order to ensure secure and interoperable interfaces between the NPSBN and external elements (e.g., all SGi, Rx and Srvs services as shown in Figure 2), these interfaces shall be protected with a FirstNet-approved security mechanism.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-44-F	User domain security shall be implemented in accordance with 3GPP TS 33.102, TS 31.101, and TS 22.022.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-45-F	USIM-based applications that require messaging between the USIM and network components shall implement application domain security in accordance with 3GPP TS 33.102 and TS 31.111.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-46-F	In such cases where visibility is required for devices on the NPSBN, the implementations shall comply with 3GPP TS 33.102 and TS 22.101.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-47-F	Hardware and software systems comprising the NPSBN should support integration of existing network elements via the necessary commercial standards-defined LTE interfaces enumerated in Table 1: Minimum Interoperable Interfaces.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-48-F	Billing information from the NPSBN should be provided to each local and/or regional entity for the NPSBN services.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-49-F	The NPSBN should support existing public safety applications, deployed regionally or within agencies.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-50-F	The NPSBN should provide a method to connect a device to a packet data network where a homepage application is hosted with location specific content.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-51-F	The NPSBN should provide a method where a homepage‖ application is available via an alternate access network, other than the NPSBN. This is a recommendation that the homepage be made available and location-aware while roaming or over Wi-Fi.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-52-F	The NPSBN should provide a specification for locating a—homepage‖ based on current or manual location.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-53-F	The NPSBN should support use of field-deployed server applications.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-54-F	The NPSBN should support devices that are reachable via the global Internet and can be used to host field based server applications (i.e., deployable servers).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-55-F	The NPSBN should allow the devices outside of their normal jurisdiction to connect to a local packet data network and to the device‘s home packet data network to carry out incident objectives.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-56-F	The NPSBN should provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-57-F	Voice sessions should be handed off within the NPSBN with limited delay and loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature is a future evolution capability.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-58-F	The NPSBN should support Voice over LTE (cellular voice) capabilities using GSMA PRD IR.92.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-59-F	The NPSBN should allow the integration of high power LTE UEs as they become available, based on the methodology contained in Table 2: Standards Implementation Methodology.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-60-F	User devices and device management solutions should support remote management capabilities over- the-air, including software update, discovery, device platform configuration, lock, unlock, wipe, and security configuration.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-61-F	The software systems that comprise the NPSBN should support the ability to enable local entities to install, update, and manage their own applications. This may include security, transport and local APN provisioning.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-62-F	The software systems that comprise the NPSBN should provide published and version-controlled subscriber provisioning interfaces to enable end-to-end subscriber provisioning by the local entities. These interfaces should be verified during interoperability testing.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-63-F	Prior to operational deployment on the NPSBN, infrastructure equipment should have passed FirstNet- required performance testing of individual interfaces, nodes and overall system as per the specific performance requirements of the NPSBN.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-64-F	Nationwide applications on the NPSBN should have passed FirstNet-required security testing to proper security levels (e.g., Criminal Justice Information Services [CJIS]) to ensure protection of FirstNet and public safety information.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-65-F	The NPSBN should allow for connection and operation of IP-based LMR voice interoperability gateways using open interfaces as they are developed.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-66-F	The NPSBN should be constructed and evolved in adherence to a multi-year roadmap.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-67-F	Infrastructure equipment procured for the NPSBN should support backwards compatibility with deployed LTE devices.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-68-F	Infrastructure equipment in the NPSBN should be upgradeable to, minimally, two major 3GPP releases (i.e., n+2, where n is the release available at deployment provided that the equipment does not need to implement a new air interface specification).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-69-F	Hardware and software systems comprising the NPSBN should support industry practices for management of standard network interfaces from each supplier. These industry practices include formal publication of interface compliance, deprecation of interfaces, support for backwards compatibility and graceful obsolescence of interfaces.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-70-F	The NPSBN should support industry practices for life cycle management of interfaces that it exposes to applications or users of the network to ensure backward compatibility for a reasonable interval, using industry- practice interface deprecation and obsolescence methods. The interfaces include, but may not be limited to: network messaging protocols, application programming interfaces, Web-based interfaces, protocol/messaging interfaces, and user interfaces such as command line interfaces.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-71-F	The EPC equipment in the NPSBN should support optional local and geographic redundancy.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-72-F	The equipment in the NPSBN should support transport redundancy wherever economically feasible (i.e., connections to local switching equipment or WAN connectivity between sites or core locations).	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-73-F	If roaming between the NPSBN and commercial LTE networks is implemented, and IP Multimedia Subsystem is implemented in the NPSBN, the NPSBN should implement support for IP Multimedia Subsystem while roaming into other LTE PLMNs.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-74-F	Coverage maps should be maintained that show pictorially which GoS tiers are supported over a geographic area. Detailed maps should be made available to authorized public safety agencies.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-75-F	NPSBN coverage maps showing planned future coverage should be maintained. The maps should show planned coverage at regular intervals (e.g., quarterly) into the future. These maps should be made available to authorized public safety agencies.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-76-F	The NPSBN should use a set of pre-defined GoS tiers to provide clear and uniform description of the services of network performance provided within a coverage area.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-77-F	The GoS tiers should include the minimum set of GoS attributes defined in Section 4.6.3.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-78-F	The expected or actual GoS tier should be disclosed to authorized public safety agencies in a geographic region.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-79-F	Each coverage area should be designed to operate with a defined GoS tier.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-80-F	Service probability should be specified for each GoS tier, in order to specify the quality of the user experience provided by the network.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-81-F	The expected minimum uplink (mobile to network) and downlink (network to mobile) rates of data transmission should be specified for each GoS tier. The specifications must also include the protocol layer at which the data rates are to be measured.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-82-F	The NPSBN should implement a scheme for engineering RAN boundaries according to a national cell coordination plan.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-83-F	A set of default QoS profile templates should be defined for each responder function (e.g., police, fire, EMS) supported by the NPSBN.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-84-F	Each QoS profile template should contain a descriptive definition of the responder function and default values for ARP, Access Class, UE-AMBR, and APN-AMBR.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-85-F	Since the NPSBN could also support secondary users, default QoS profile templates should be defined for public safety and secondary users.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-86-F	Every user of the NPSBN (public safety and secondary users) should be assigned a default prioritization and QoS profile using the set of pre-defined QoS profile templates.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-87-F	A process should be established and followed to manage the assignment of templates to users to ensure template assignment rules are uniformly applied for all users using the NPSBN.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-88-F	FirstNet should make an API available to national, regional, and local applications to expose Priority and QoS control.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-89-F	The NPSBN security implementation should include pre-planned bypass mechanisms that have defined security and interoperability implications.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-90-F	Equipment used in the NPSBN should support AES and SNOW 3G algorithms.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-91-F	FirstNet should establish the security controls and policy for inter-domain security and require that all parties (e.g., public safety agencies) that connect to the NPSBN utilize FirstNet-approved cipher suites.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-92-F	FirstNet should consider using IPSec interfaces that utilize IKEv2 and utilize PKI to authenticate the peers of the IPSec security associations.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-93-F	When EPS elements are located in trusted locations without wide area communication links between them, the use of network domain security should be optional.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-94-F	Network interfaces between domains should be monitored and intrusion detection/prevention tools should be deployed.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-95-F	The developed security mechanisms should permit local entities to hide the topologies and address spaces of their networks.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-96-F	Security mechanisms layered by a jurisdiction on top of the NPSBN should not inhibit interoperability for users visiting from outside of the security domain in which it is implemented.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

Statement of Objective/ FCC TAB Item	Item Summary	IOC and/or FOC Milestone to be Validated In
FCC-001-97-F	As FirstNet enters into roaming agreements with commercial partners, security policies should be implemented that ensure integrity of the NPSBN and ensure that NPSBN security practices are not compromised.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-98-F	FirstNet should consider supporting implementation of a national framework for user identity management.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-99-F	FirstNet should consider supporting implementation of a national framework for user identity federation to enable user interoperability across administrative domains within the NPSBN, where authorized.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-100-F	Implementation of the national framework for user identity management and federation should include a set of guidelines and rules for applications to participate in the national identity management framework.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*
FCC-001-101-F	The agency, organization or entity that utilizes the NPSBN identity management framework should be responsible for enforcing authorization constraints on access to information as per their own security policy.	*< List IOC/FOC phase this SOO or FCC TAB item will be validated. Example: IOC-1, IOC-2, IOC-5 and FOC and/or any combination.>*

2.1.1 User Equipment Test Strategy

<Describe the UE test strategy here. Topics to address include but are not limited to UE certification, UE-RAN Interoperability (IOT), Wi-Fi Connectivity, Bluetooth Connectivity, Battery Certification, Carrier Acceptance Testing, etc.>

2.1.2 RAN Test Strategy

<Describe the RAN test strategy here. Topics to address include but are not limited to conformance testing, commissioning, certification testing, RAN-EPC IOT testing, backhaul testing, how Band 14 coverage objectives specified in the IOC/FOC Target Timeline (Section J, Attachment J-8) will be tested, how hardening and resiliency will be tested, etc. >

2.1.3 EPS and IP Multimedia Subsystem Test Strategy

<Describe the EPS and IP Multimedia Subsystem test strategy here. Topics to address include but are not limited to sub-system testing, EPS and IP Multimedia Subsystem interface conformance testing, EPS and IP Multimedia Subsystem load testing, EPS and IP Multimedia Subsystem vulnerability testing, how hardening and resiliency will be tested, etc.>

2.1.4 Network Services Test Strategy

<Describe the Network Services test strategy here. Topics to address include but are not limited to Location-Based Services (LBS) testing, messaging services (SMS, MMS) testing, and VoLTE and RCS testing.>

2.1.5 Application Test Strategy

<Describe the Application test strategy here. Topics to address include but are not limited to application certification; application testing; Mobile Device Management server functionality; application security testing; federated Identity, Credential, and Access Management (ICAM) testing; application resiliency testing; application interaction testing; application performance testing; application/device interoperability testing; application battery life testing; application infrastructure testing; application server load testing; etc.>

2.1.6 Operational Support System and Business Support System Test Strategy

<Describe the OSS and BSS test strategy here. Topics to address include but are not limited to alarming, alarm management, billing, etc.>

<As part of the OSS and BSS test strategy, describe creation, maintenance, and support of a network operation connection and quality assurance monitoring of FirstNet NPSBN performance Key Performance Indicators (KPIs) at the FirstNet technical headquarters.>

2.1.7 End to End Regression Test Strategy

<Describe the end-to-end regression test strategy here. Topics to address include overall end-to-end regression testing for each IOC and FOC, etc.>

2.2 Interim Operational Capability (IOC) Test

2.2.1 IOC-1

< Describe the IOC-1 test configurations for the laboratory, field, and First Office Application (FOA). The Offeror should show how select Public Safety Enterprise Network (PSEN) configuration(s) will be included in the FOA. Provide high-level block diagrams for each test configuration.

Describe the entrance criteria to IOC-1 by completing the table below. IOC-1 testing can not begin until the entrance criteria are met. Also, as part of the entry criteria, describe what test reports are required before performing this IOC.>

Table 2 IOC-1 Entry Criteria

Entry Criteria	Description
<Example: IOC-1 System Level Test Plans/Procedures>	*<Example: Test plans and procedures have been reviewed, accepted, and are available.>*
<Example: Software Release>	*<Example: General Availability (GA) Quality Software Load with X% System Test Pass Rate>*
<Example: Defect Report>	*<Example: List of outstanding high severity defects and timeline as to when the defects will be resolved.>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*
<…>	*<…>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*

<Describe how each item that was identified as being tested in IOC-1 in Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones above will be verified by completing the table below.>

Table 3 IOC-1 Description of Verification Strategy Per Item

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other = TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.
<…>	*<…>*	*<…>*

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other = TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.

<Describe the exit criteria for IOC-1 by completing the table below.>

Table 4 IOC-1 Exit Criteria

Exit Criteria	Description	Projected Availability
<Example: IOC-1 Testing Complete>	*<Example: IOC-1 Final Test Report. This final test report will be composed of three separate reports for each of the three test environments (lab, field, and FOA). Offeror(s) will create the initial draft IOC-1 test report and submit to FirstNet for comment and review. In each test report, Offeror(s) will clearly summarize which test cases passed or failed and any outstanding defects.>*	*<Example: 30 days after test completion>*
<Example: IOC-1 Final Defect Report>	*<Example: Offeror(s) to summarize the remaining critical, major, minor defects and proposal to resolve outstanding defects.>*	*<Example: 30 days after test completion>*
<…>	*<…>*	*<…>*
<Add exit criteria here>	*<Add exit criteria description here>*	*<Add projected availability here>*

2.2.2 IOC-2

<Describe the IOC-2 test configurations for the laboratory, field, and FOA. The Offeror should show how select PSEN configuration(s) will be included in the FOA. Provide high-level block diagrams for each test configuration.

Describe the entrance criteria to IOC-2 by completing the table below. IOC-2 testing can not begin until the entrance criteria is met. Also, as part of the entry criteria, describe what test reports are required before performing this IOC.>

Table 5 IOC-2 Entry Criteria

Entry Criteria	Description
<Example: IOC-2 System Level Test Plans/Procedures>	*<Example: Test plans and procedures have been reviewed, accepted, and are available.>*
<Example: Software Release>	*<Example: General Availability (GA) Quality Software Load with X% System Test Pass Rate>*
<Example: Defect Report>	*<Example: List of outstanding high severity defects and timeline as to when the defects will be resolved.>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*
<…>	*<…>*

Entry Criteria	Description
<Add additional entry criteria items here>	*<Add description of entry criteria here>*

<Describe how each item that was identified as being tested in IOC-2 in Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones above will be verified by completing the table below.>

Table 6 IOC-2 Description of Verification Strategy Per Item

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other = TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.
<…>	*<…>*	*<…>*
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.

<Describe the exit criteria for IOC-2 by completing the table below.>

Table 7 IOC-2 Exit Criteria

Exit Criteria	Description	Projected Availability
<Example: IOC-2 Testing Complete>	*<Example: IOC-2 Final Test Report. This final test report will be composed of three separate reports for each of the three test environments (lab, field, and FOA). Offeror(s) will create the initial draft IOC-2 test report and submit to FirstNet for comment and review. In each test report, the Offeror will clearly summarize which test cases passed or failed and any outstanding defects.>*	*<Example: 30 days after test completion>*
<Example: IOC-2 Final Defect Report>	*<Example: Offeror(s) to summarize the remaining critical, major, minor defects and proposal to resolve outstanding defects.>*	*<Example: 30 days after test completion>*
<…>	*<…>*	*<…>*
<Add exit criteria here>	*<Add exit criteria description here>*	*<Add projected availability here>*

2.2.3 IOC-3

<Describe the IOC-3 test configurations for the laboratory, field, and FOA. The Offeror should show how select PSEN configuration(s) will be included in the FOA. Provide high-level block diagrams for each test configuration.

Describe the entrance criteria to IOC-3 by completing the table below. IOC-3 testing can not begin until the entrance criteria is met. Also, as part of the entry criteria, describe what test reports are required before performing this IOC.>

Table 8 IOC-3 Entry Criteria

Entry Criteria	Description
<Example: IOC-3 System Level Test Plans/Procedures>	*<Example: Test plans and procedures have been reviewed, accepted, and are available.>*
<Example: Software Release>	*<Example: General Availability (GA) Quality Software Load with X% System Test Pass Rate>*
<Example: Defect Report>	*<Example: List of outstanding high severity defects and timeline as to when the defects will be resolved.>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*
<…>	*<…>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*

<Describe how each item that was identified as being tested in IOC-3 in Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones above will be verified by completing the table below.>

Table 9 IOC-3 Description of Verification Strategy Per Item

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other = TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.
<…>	*<…>*	*<…>*
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.

<Describe the exit criteria for IOC-3 by completing the table below.>

Table 10 IOC-3 Exit Criteria

Exit Criteria	Description	Projected Availability
<Example: IOC-3 Testing Complete>	*<Example: IOC-3 Final Test Report. This final test report will be composed of three separate reports for each of the three test environments (lab, field, and FOA). Offeror(s) will create the initial draft IOC-3 test report and submit to FirstNet for comment and review. In each test report, the Offeror will clearly summarize which test cases passed or failed and any outstanding defects.>*	*<Example: 30 days after test completion>*
<Example: IOC-3 Final Defect Report>	*<Example: Offeror(s) to summarize the remaining critical, major, minor defects and proposal to resolve outstanding defects.>*	*<Example: 30 days after test completion>*
<…>	*<…>*	*<…>*
<Add exit criteria here>	*<Add exit criteria description here>*	*<Add projected availability here>*

2.2.4 IOC-4

<Describe the IOC-4 test configurations for the laboratory, field, and FOA. The Offeror should show how select PSEN configuration(s) will be included in the FOA. Provide high-level block diagrams for each test configuration.

Describe the entrance criteria to IOC-4 by completing the table below. IOC-4 testing can not begin until the entrance criteria is met. Also, as part of the entry criteria, describe what test reports are required before performing this IOC.>

Table 11 IOC-4 Entry Criteria

Entry Criteria	Description
<Example: IOC-4 System Level Test Plans/Procedures>	*<Example: Test plans and procedures have been reviewed, accepted, and are available.>*
<Example: Software Release>	*<Example: General Availability (GA) Quality Software Load with X% System Test Pass Rate>*
<Example: Defect Report>	*<Example: List of outstanding high severity defects and timeline as to when the defects will be resolved.>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*
<…>	*<…>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*

<Describe how each item that was identified as being tested in IOC-4 in Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones above will be verified by completing the table below.>

Table 12 IOC-4 Description of Verification Strategy Per Item

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other=TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.
<…>	*<…>*	*<…>*
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.

<Describe the exit criteria for IOC-4 by completing the table below.>

Table 13 IOC-4 Exit Criteria

Exit Criteria	Description	Projected Availability
<Example: IOC-4 Testing Complete>	*<Example: IOC-4 Final Test Report. This final test report will be composed of three separate reports for each of the three test environments (lab, field, and FOA). Offeror(s) will create the initial draft IOC-4 test report and submit to FirstNet for comment and review. In each test report, the Offeror will clearly summarize which test cases passed or failed and any outstanding defects.>*	*<Example: 30 days after test completion>*
<Example: IOC-4 Final Defect Report>	*<Example: Offeror(s) to summarize the remaining critical, major, minor defects and proposal to resolve outstanding defects.>*	*<Example: 30 days after test completion>*
<…>	*<…>*	*<…>*
<Add exit criteria here>	*<Add exit criteria description here>*	*<Add projected availability here>*

2.2.5 IOC-5

<Describe the IOC-5 test configurations for the laboratory, field, and FOA. The Offeror should show how select PSEN configuration(s) will be included in the FOA. Provide high-level block diagrams for each test configuration.

Describe the entrance criteria to IOC-5 by completing the table below. IOC-5 testing can not begin until the entrance criteria are met. Also, as part of the entry criteria, describe what test reports are required before performing this IOC.>

Table 14 IOC-5 Entry Criteria

Entry Criteria	Description
<Example: IOC-5 System Level Test Plans/Procedures>	*<Example: Test plans and procedures have been reviewed, accepted, and are available.>*
<Example: Software Release>	*<Example: General Availability (GA) Quality Software Load with X% System Test Pass Rate>*
<Example: Defect Report>	*<Example: List of outstanding high severity defects and timeline as to when the defects will be resolved.>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*
<…>	*<…>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*

<Describe how each item that was identified as being tested in IOC-5 in Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones above will be verified by completing the table below.>

Table 15 IOC-5 Description of Verification Strategy Per Item

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other=TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.
<…>	*<…>*	*<…>*
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.

<Describe the exit criteria for IOC-5 by completing the table below.>

Table 16 IOC-5 Exit Criteria

Exit Criteria	Description	Projected Availability
<Example: IOC-5 Testing Complete>	*<Example: IOC-5 Final Test Report. This final test report will be composed of three separate reports for each of the three test environments (lab, field, and FOA). Offeror(s) will create the initial draft IOC-5 test report and submit to FirstNet for comment and review. In each test report, the Offeror will clearly summarize which test cases passed or failed and any outstanding defects.>*	*<Example: 30 days after test completion>*
<Example: IOC-5 Final Defect Report>	*<Example: Offeror(s) to summarize the remaining critical, major, minor defects and proposal to resolve outstanding defects.>*	*<Example: 30 days after test completion>*
<…>	*<…>*	*<…>*
<Add exit criteria here>	*<Add exit criteria description here>*	*<Add projected availability here>*

2.3 Final Operational Capability (FOC) Test

<FOC test is intended to evaluate the readiness for the FirstNet service offering to deliver the final operational capability planned for the NPSBN. This final operational capability test stage will review various aspects of FCC TAB and SOO as final verification that all required system features and functionality have been delivered.

Describe the FOC test configurations for the laboratory, field, and FOA. The Offeror should show how select PSEN configuration(s) will be included in the FOA. Provide high-level block diagrams for each test configuration.

Describe the entrance criteria to FOC by completing the table below. FOC testing can not begin until the entrance criteria are met. Also, as part of the entry criteria, describe what test reports are required before performing this FOC.>

Table 17 FOC Entry Criteria

Entry Criteria	Description
<Example: FOC System Level Test Plans/Procedures>	*<Example: Test plans and procedures have been reviewed, accepted, and are available.>*
<Example: Software Release>	*<Example: General Availability (GA) Quality Software Load with X% System Test Pass Rate>*
<Example: Defect Report>	*<Example: List of outstanding high severity defects and timeline as to when the defects will be resolved.>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*
<…>	*<…>*
<Add additional entry criteria items here>	*<Add description of entry criteria here>*

<Describe how each item that was identified as being tested in FOC in Table 1 FirstNet Statement of Objectives and FCC TAB Item Mapping to IOC/FOC Milestones above will be verified by completing the table below.>

Table 18 FOC Description of Verification Strategy Per Item

Statement of Objective/FCC TAB Item #	Description of Verification Strategy	Test Location (OL = Offeror Lab; OF = Offeror Field; PSEN = PS Enterprise Network; FNL = FirstNet Lab; Other=TBD by Offeror)
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.
<…>	*<…>*	*<…>*
<Add SOO Section #/FCC TAB Item # here>	*<Add brief verification strategy here>* 1. *<Add verification items for this SOO/FCC TAB item here in number bullet form>* 2.	*<Identify Test Location Per Verification Strategy>* 1. *<Add Test Location(s) OL, OF, PSEN, FNL, and/or Other for each verification item>* 2.

<Describe the exit criteria for FOC by completing the table below.>

Table 19 FOC Exit Criteria

Exit Criteria	Description	Projected Availability
<Example: FOC Testing Complete>	*<Example: FOC Final Test Report. This final test report will be composed of three separate reports for each of the three test environments (lab, field, and FOA). Offeror(s) will create the initial draft FOC test report and submit to FirstNet for comment and review. In each test report, the Offeror will clearly summarize which test cases passed or failed and any outstanding defects.>*	*<Example: 30 days after test completion>*
<Example: FOC Final Defect Report>	*<Example: Offeror(s) to summarize the remaining critical, major, minor defects and proposal to resolve outstanding defects.>*	*<Example: 30 days after test completion>*
<…>	*<…>*	*<…>*
<Add exit criteria here>	*<Add exit criteria description here>*	*<Add projected availability here>*

2.4 Post FOC Testing

<Once FOC testing has been completed, FirstNet will reach a stable state where it carries out daily operations, which is referred to as "Post FOC." The purpose of this section is for the Offeror to describe the Post FOC testing strategy including but not limited to regression testing, new feature testing, FOA testing, Radio Frequency (RF) system optimization, carrier acceptance of new devices, carrier acceptance

of new applications, etc. In addition, the Offeror should consider describing their approach to performing quality assurance and surveillance on the operational network.>

3 Test Strategy Schedule and Test Management

3.1 Test Planning and Execution Schedule

<The Offeror to describe how FirstNet would be included in IOC and FOC test plan and procedure reviews and the frequency of such reviews. The Offeror also to describe the IOC and FOC test planning and execution timeline in the form of a Gantt Chart, which includes test plan development, procedure reviews, and test execution.>

3.2 Test Data Management

<The Offeror to briefly describe how test data (test case results) will be archived and preserved for each IOC, FOC, and post-FOC. This includes discussing the data retention policy.>

4 Equipment, Test Tools, and Training

<The Offeror to describe network equipment, test equipment, test tools, and training to be provided per IOC/FOC in the Offeror Lab (OL), Offeror Field (OF) Environment, at the PSEN, and in the FirstNet laboratory in Boulder, Colorado, including:

- *Installation and configuration of any hardware, software and test tools necessary to execute public safety feature acceptance test plans and cases.*
- *Hardware and software installation, upgrades, configuration, maintenance, licensing, and repair of the Offeror's installed or interconnected lab equipment.*
- *Maintenance plan for current and spare equipment inventory for the Offeror's installed or interconnected lab equipment.*
- *Training and support for FirstNet staff to execute FirstNet's own public safety feature quality assurance test plan.>*

Table of Contents

1 Document Overview

This document contains the terms of reference that FirstNet may use in the solicitation and associated documents. In the case of any conflict in terms used throughout this RFP, the terms of reference set forth in this Section J Attachment J-14 Terms of Reference shall take precedence in resolution.

2 Terms of Reference

Term	Definition
3GPP	The 3rd Generation Partnership Project (3GPP) is a collaboration among telecommunications associations known as the Organizational Partners. The initial scope of 3GPP was to make a globally applicable third-generation (3G) mobile phone system specification based on evolved Global System for Mobile Communications (GSM) specifications within the scope of the International Mobile Telecommunications-2000 project of the International Telecommunication Union. The scope was later enlarged to include the development and maintenance of: • GSM and related 2G and 2.5G standards, including GPRS and EDGE • UMTS and related 3G standards including HSPA • Long Term Evolution and related 4G standards • An evolved IMS developed in an access-independent manner
ABAC	Attribute-based access control defines an access control paradigm whereby access rights are granted to users through the use of policies that combine attributes together. The policies can use any type of attributes (e.g., user attributes, resource attributes, environment attributes).
Access Class Barring	Within, 3GPP, Access Class Barring requires that the user equipment be a member of at least one Access Class that corresponds to the permitted classes as signaled over the air interface.
ADNSF	Access network discovery and selection function is an entity within an evolved packet core (EPC) of the system architecture evolution (SAE) for 3GPP compliant mobile networks. The purpose of the ANDSF is to assist user equipment (UE) to discover non-3GPP access that can be used for data communications in addition to 3GPP access networks (such as HSPA or LTE) and to provide the UE with rules policing the connection to these networks.
Analog	Analog refers to anything relating to or using signals or information represented by a continuously variable physical quantity such as spatial position or voltage.
API	An Application Programming Interface specifies a software component in terms of its operations, inputs, outputs, and underlying types. It is used to provide a basis for accessing, controlling, or utilizing the component.
APN	An Access Point Name is the name of a gateway between a GPRS, 3G, or 4G mobile network and another computer network, frequently the public Internet. A mobile device making a data connection must be configured with an APN to present to the carrier. The carrier will then examine this identifier to determine what type of network connection should be created—for example, which IP addresses should be assigned to the wireless device; which security methods should be used; and how, or if, it should be connected to a private customer network.

Term	Definition
Application	An application is a software program or group of programs designed to perform an activity or enterprise function. Applications can exist on mobile devices, workstations, or servers. General-purpose applications include items such as database programs, word processors, Web browsers, and spreadsheets. Applications for public safety users address topics such as situational awareness, incident management, and interoperable communications.
Applications Ecosystem	An innovative set applications along with the supporting ecosystem, such as a development and testing environment, an app store, and vibrant developer community.
ARP	Allocation Retention Priority specifies the relative importance compared to other Radio access bearers for allocation and retention of the radio access bearer.
ATIS	The Alliance for Telecommunications Industry Solutions is a standards organization that develops technical and operational standards and solutions for the information and communications technology industry.
AVL	Automatic Vehicle Location systems typically locate and track vehicles using GPS, and the transmission mechanism is SMS, GPRS, a satellite, or terrestrial radio from the vehicle to a radio receiver. This data, from one or more vehicles, may then be collected by a vehicle tracking system for a picture of vehicle travel.
Backhaul	In the NPSBN, the backhaul portion of the network comprises the links from the cell sites (eNodeBs) to the Offeror-defined consolidation/aggregation points for the transport network which will in-turn carry that traffic to the core.
Band 14	A commercial Long Term Evolution frequency range of 20 (10 X 10) MHz of spectrum in the 700 MHz band dedicated to public safety. Specifically, 788 – 798 MHz for the uplink (handset/UE transmit) and 758 – 768 for the downlink (base station transmit).
BSS	Business support systems are the components that a telecommunications service provider (or telco) uses to run its business operations towards customers. Together with operational support systems, they are used to support various end-to-end telecommunication services (e.g., telephone services).
BYOD	Bring Your Own Device is the practice of allowing users to utilize a personally selected and purchased client device to execute applications and access data. Typically, it spans laptops, smartphones and tablets, but the strategy may also be used for other devices.
CAD	Computer Aided Dispatch typically consists of a suite of software packages used to initiate public safety response, dispatch, and to maintain the status of responding resources in the field. It is generally used by emergency communications dispatchers, call-takers, and 911 operators in centralized, public-safety call centers, as well as by field personnel.
CALEA	Communications Assistance for Law Enforcement Act is the United States wiretapping law passed in 1994, during the presidency of Bill Clinton (Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010). CALEA's purpose is to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to wiretap any telephone traffic; it has since been extended to cover broadband internet and VoIP traffic.
CAR	A Corrective Action Report is a written request used to originate a corrective action. It is used as a response to a defect with the intent to eliminate the problem from occurring again. The main objective of a CAR is to initiate a root cause analysis and request a resolution to prevent recurrence.
CATL	CTIA Authorized Test Labs is a device-testing laboratory that meets the Policies and Procedures for CTIA Authorized Testing Laboratories, Revision 1.4 August 2015 and is listed as such by the CTIA.

Term	Definition
CJIS	Criminal Justice Information Services is a repository of information operated by the FBI containing crime data such as records and non-crime data such as fingerprints as well as a variety of other information of use to law enforcement.
CLA	A Covered Leasing Agreement as defined under the Act at 47 U.S.C. 1422(b)(1) as further interpreted by FirstNet's Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012 [Docket Number: 140821696-4696-01], published October 20, 2015. The terms of the CLA shall be incorporated into the Covered Agreement resulting from this RFP.
CLA User	See Secondary User
Client Server Application	A Client Server Application is one that has a user interface (UI) on the UE but requires a network interface to servers to performs many/most of its essential functions
Client-Only Application	A Client-only Application is one that runs on the UE and requires no network connection to perform all of its essential functions
CMAS	Commercial Mobile Alert System is an alerting network in the United States designed to disseminate emergency alerts to mobile devices such as cell phones and pagers. Now known as WEA.
CO	Contracting Officer is a person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings
COML	The Communications Unit Leader heads the communications unit and is responsible for integrating communications and ensuring that operations are supported by communications.
Contractor	The awardee of the Covered Agreement resulting from this RFP.
COR	The Contracting Officer's Representative is an individual, including a Contracting Officer's Technical Representative, who is designated and authorized in writing by the Contracting Officer to perform specific technical or administrative functions
Core	The Core Network as defined under the Act at 47 U.S.C. 1422(b)(1) as further interpreted by FirstNet's Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012 [Docket Number: 140821696-4696-01], published October 20, 2015.
COTR	Contracting Officer Technical Representative is a business communications liaison between the United States government and a private contractor. See COR.
COTS	Commercial Off The Shelf refers to software that can be purchased or licensed that contains all or most of the functionality required by the customer. COTS software often times requires configuration and/or customization to bridge the gap between what is received from the vendor to reach the 100% of functionality.
Coverage	The geographic area where a base station and mobile device can reliably communicate with each other above a minimum designed data rate.
Covered Agreement	The agreement that ultimately results from this RFP, which covers all terms and conditions related to the deployment and operation of the NPSBN, including those terms regarding spectrum capacity usage.
COWs	A Cell On Wheels is a mobile cell site that consists of a cellular antenna tower and electronic radio transceiver equipment on a truck or trailer, designed to be part of a cellular network. COWs are used to provide expanded cellular network coverage and/or capacity at special events such as major sporting events, or in disaster areas where cellular coverage either was never present (e.g., in a wilderness area) or was compromised by the disaster (e.g., in the Gulf Coast after Hurricane Katrina).
CPARS	Contractor Performance Assessment Reporting System is a web-enabled application that collects and manages the library of automated CPARs. A CPAR assesses a contractor's performance and provides a record, both positive and negative, on a given contractor during a specific period of time.

Term	Definition
CRM	Customer Relationship Management is formal approach to managing an organization's interaction with current and future customers. It often involves using information technology to organize, automate, and synchronize sales, marketing, customer service, and technical support activity.
CTIA	The Wireless Association, originally known as the Cellular Telephone Industries Association, is an international industry trade group representing all wireless communication sectors including cellular, personal communication services, and enhanced specialized mobile radio.
Customer Life-Cycle Management	The functions associated with providing the full suite of customer lifecycle activities required to service Public Safety customers effectively including, but not limited to, product and services sales and distribution, marketing, customer care, billing, product management, product development, end-user device logistics, churn mitigation, and special pricing support.
Customer-Facing Web-Based Portal	The customer-facing Web-based portal is a set of Web pages where Nationwide Public Safety Broadband Network subscribers can view and purchase services plans, devices, etc.
Cybersecurity Incident	Any malicious act or suspicious event that (1) compromises, or was an attempt to compromise, the electronic security perimeter or physical security perimeter of a critical cyber asset, or (2) disrupts, or was an attempt to disrupt, the operation of a critical cyber asset where a critical cyber asset is any hardware, firmware, software, or related component or subcomponent critical to the operational and functional capability of the cyber system in question.
DAST	Dynamic Analysis Security Testing encompasses the technologies and tools that are used for security vulnerabilities when the applications are being executed.
DDoS	Distributed Denial of Service is where the attack source is more than one – and often thousands – of unique IP addresses.
Delivery Mechanism for State Plans	The delivery mechanism for state plans is a state plan Web-based online delivery tool that will house the details of all sections of the state plan, with mediated and secure access, and will be the means by which each state reviews its state plan.
Deployable	Transportable equipment principally in a vehicle to provide network services to users when augmenting network capacity or coverage is required for planned or unplanned events. Intended primarily for remote and wilderness areas where little infrastructure exists or areas where existing infrastructure has been compromised.
Device(s)	A device accesses the network, and may be as simple as a small modem for machine-to-machine use or as complex as a smartphone or tablet. Devices can provide direct interfaces for first responders, such as a smartphone would, or they can be a gateway to the network for another device, such as the modems in vehicles that let mobile data terminals access the network.
DHS	Department of Homeland Security is a cabinet department of the United States federal government with the primary responsibilities of protecting the territory of the United States and protectorates from and responding to terrorist attacks, man-made accidents, and natural disasters.
DIVV	Device Independent Verification and Validation is the process by which FirstNet envisions ensuring devices allowed on the Nationwide Public Safety Broadband Network are in compliance and meet the needed performance for Public Safety focused features and functions. This is similar to what is known as carrier acceptance testing in industry.
DM	Device Management is a system of client/server applications that allows an enterprise to remotely control, lock, and enforce security policies on the devices on their network. Mobile Device Management is the same term.

Term	Definition
DOC	Department of Commerce is a cabinet department in the U.S. Government that supports and promotes business, trade and commerce.
DoS	Denial of Service is an attack that attempts to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
DRA	Diameter Routing Agent is a functional element that ensures that all Diameter sessions for a certain IP connectivity access network IP-CAN session reach the same PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm.
DSCP	Differentiated Services Code Point is a computer networking architecture that specifies a simple, scalable, and coarse-grained mechanism for classifying and managing network traffic and providing QoS on modern IP networks. DiffServ can, for example, be used to provide low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.
eICIC	Enhanced Inter cell Interference Coordination is defined in 3GPP Rel 10
Embedded Application	An embedded application is included in the native OS of the UE. An embedded application often provides a UI for a lower level function within the device but may also be a client-only (calculator) or client-server (PTT client).
eMBMS	Evolved Multimedia Broadcast Multicast Service is the LTE version of MBMS.
EMS	An Element Management System manages one or more of a specific type of telecommunications network element. Typically, an EMS is produced and distributed by a manufacturer to manage one or more of their products. EMS has another definition so use of the acronym is avoided.
EMS	Emergency Medical Services is a major category of Public Safety users focused on health and welfare services. EMS is often a part of Fire and Rescue services. EMS has another definition so use of the acronym is avoided.
eNB	Enhanced Node Base station or eNodeB is base station hardware connected to the mobile network that communicates directly with mobile devices; this is similar to a Base Transceiver Station (BTS) in GSM networks. Traditionally, a Node B has minimum functionality, and is controlled by an RNC (Radio Network Controller). However, with an eNB, there is no separate controller element. This simplifies the architecture and allows faster response times.
Enhanced LTE Public Safety Grade Voice Telephony	Enhanced LTE Public Safety Grade voice telephony refers to VoLTE on a Public Safety Grade network with the added capabilities of QPP and secure applications. It may also include enhancements (as described in Section J, Attachment J-8, IOC/FOC Target Timeline, Section 3.3.2.1, Services) for 3GPP Releases 13 and 14 that are expected to be implemented by the Offeror.
EPC	Evolved Packet Core. The main component of the SAE architecture is the EPC, also known as SAE Core. The EPC will serve as the equivalent of GPRS networks (via the MME, S-GW, and P-GW subcomponents).
EPS	Evolved Packet System (EPS). Introduced with 3GPP Release-8 with SAE, the EPS is the central network portion of the LTE mobile communication system. The packet system primarily transfers packet data between edge networks and the Radio Access Network.
E-RAB	E-UTRAN Radio Access Bearer (E-RAB) uniquely identifies the concatenation of an S1 Bearer and the corresponding Data Radio Bearer. When an E-RAB exists, there is a one-to-one mapping between this E-RAB and an EPS bearer of the Non Access Stratum.

Term	Definition
ERP	ERP is Effective Radiated Power. It is the power supplied to an antenna multiplied by the antenna gain in a given direction.
ESInet	The NG911 vision relies on 911-specific application functionality on an Emergency Services IP Network (ESInet) to deliver voice, video, text, and data "calls" to the Public Safety Answering Point.
Excess Network Capacity	Excess network capacity is defined as capacity not used by Public Safety Entities (PSEs). Under the Act, FirstNet may receive payment for its use.

Term	Definition
Extended Primary User Group	The extended primary user group consists of other PSE users—beyond law enforcement, fire, and emergency medical services.
FAR	Federal Acquisition Regulation is the principal set of rules in the Federal Acquisition Regulation System. The FAR System governs the "acquisition process" by which the United States federal government purchases (acquires) goods and services.
FCAPS	Fault, Configuration, Accounting, Performance and Security is the ISO Telecommunications Management Network model and framework for network management.
FCC	Federal Communications Commission is the U.S. government agency with general regulatory authority over elements of the communications industry.
FCC TAB RMTR	The Act established within the FCC an advisory board to create minimum interoperability requirements for the NPSBN. The Technical Advisory Board (TAB) for First Responder Interoperability issued these requirements in 2012 in a report entitled *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network* (FCC TAB RMTR). References to the FCC TAB RMTR throughout this RFP refer to the original report adopted on June 21, 2012, by the FCC and the associated clarification issued by the TAB and received by the FCC on June 6, 2012. This is also referenced in the FCC's transmittal on June 21, 2012.
FEMA	The Federal Emergency Management Agency is an agency of the Department of Homeland Security whose mission is to support citizens and first responders to build, sustain, and improve the capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.
FICAM	Federal Identity, Credential, and Access Management comprises the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-personnel entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an agency's resources.
FIDO	Fast Identity Online Alliance is an industry consortium to address the lack of interoperability among strong authentication devices and the problems users face creating and remembering multiple usernames and passwords.
FIPS	The Federal Information Processing Standard (FIPS) Publication is a U.S. government computer security standard used to accredit cryptographic modules. The National Institute of Standards and Technology issued the FIPS Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components.
FirstNet	The First Responder Network Authority is an independent government authority with a mandate to ensure the deployment and operation of the national public safety broadband network (NPSBN).
FirstNet-Deployed RAN	A FirstNet-deployed RAN refers to a Radio Access Network (RAN) that FirstNet is responsible for deploying. This occurs when a state or territory does not elect, or is not authorized, to conduct its own deployment of a RAN in such state or territory in accordance with 47 U.S.C. 1442(e)(2)(A).
FOB	Free On Board refers to the point at which the seller transfers ownership of goods to the buyer.
FOC	Final Operational Capability is the activity has reached full maturity with all users able to exercise all intended capabilities as defined in the applicable statement(s) of work.
GB	A gigabyte is a unit of computer information equal to 1,073,741,824 bytes.

Term	Definition
GBR	Guaranteed Bit Rate is used to ensure that bearer traffic in LTE networks is appropriately handled; a mechanism is needed to classify the different types of bearers into different classes, with each class having appropriate QoS parameters for the traffic type. Examples of the QoS parameters include GBR or non-GBR, Priority Handling, Packet Delay Budget and Packet Error Loss rate. This overall mechanism is called QCI.
GCSE	Group Communication System Enablers. These support group communication service intended to provide a fast and efficient mechanism to distribute the same content to multiple users in a controlled manner.
GFIPM	GFIPM is a resource for information about the Global Federated Identity and Privilege Management program, which seeks to develop secure, scalable, and cost-effective technologies for information sharing within the law enforcement and criminal justice communities.
Government	The United States Government. When used in this RFP, it shall also refer to FirstNet or DOI ACQ, as appropriate given the context, as the representative of the United States Government responsible for this RFP.
GPRS	General packet radio services, a technology for radio transmission of small packets of data, especially between mobile phones and the Internet.
GPS	Global Positioning System. A space-based navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
GSMA	GSMA is the current name for the industry group that defines mobile network operator business and technical practices. It originally stood for Groupe Speciale Mobile Association.
GWCN	Gateway Core Network. A network sharing configuration in 3GPP in which the MME is also shared by the core network operators (in addition to the RAN, as in MOCN).
HetNet	Heterogeneous networks (HetNet) leverage macro cells, small cells, and integrated Wi-Fi network elements to extend coverage, handoffs, and interference mitigation between network elements to deliver a seamless mobile experience
HIPAA	HIPAA is the Health Insurance Portability and Accountability Act of 1996 which defines how covered entities use individually-identifiable health information or the PHI (Personal Health Information).
HSS	The Home Subscriber Server in the EPC, it is the user database that stores subscription related information to support other call control and session management entities.
Hybrid Application	A Hybrid application is one that is both a client only and a client server application. However, when running without an internet connection it may perform only a subset of its complete functional scope, but is still useful to some degree in this operational mode.
IaaS	Infrastructure as a Service - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
IAST	Interactive Analysis Security Testing is the combination of SAST and DAST on finding and mitigating software vulnerabilities in real-time.
ICAM	Identity, Credential, and Access Management is a framework for standardizing and integrating the management of identity information, credentials, and secure access to buildings, networks, and information technology systems.

Term	Definition
ICS	The Incident Command System (ICS) is a standardized approach to the command, control, and coordination of emergency response providing a common hierarchy within which responders from multiple agencies can be effective. ICS consists of a standard management hierarchy and procedures for managing a temporary incident of any size.
IdaaS	Identity-as-a-Service is a cloud-based solution for operating the information resources required by an organization specifically related to identity management of an organization.
IMS	IP Multimedia Subsystems is an architectural framework for delivering IP multimedia to mobile users. It was originally designed by the wireless standards body 3GPP, and is part of the vision for evolving mobile networks beyond GSM. IMS has another definition as well, so usage is generally avoided in the RFP documents.
IMS	Integrated Master Schedule. IMS has another definition as well, so usage is generally avoided in the RFP documents.
IMSI	International Mobile Subscriber Identity (IMSI) identifies the SIM card on a 3GPP network. The IMSI maximum length is 15 digits, and is physically stored on the SIM card. The IMSI specification includes the mobile country code, mobile network code, and mobile station identification number.
Inherently Governmental	An inherently governmental function is defined as any function related to the public interest that mandates performance by government employees.
Interoperability Board Report	Recommendations of a panel created by the Federal Communications Commission concerning specifications and technical requirements for the Nationwide Public Safety Broadband Network. Also referred to as the TAB report or the FCC TAB RMTR..
IOC	Initial Operational Capability is the state achieved when a capability is available in its minimum usefully deployable form as defined in the statement of work.
IOPS	Isolated E-UTRAN Operation for Public Safety
IoT	Internet of Things is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data.
IPAWS	Integrated Public Alert and Warning System. A planned modernization and integration of the United States emergency population warning systems.
ISDN	Integrated Services for Digital Network is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network.
ISO	International Organization for Standardization is responsible for the ISO 9000, ISO 14000, ISO 27000, ISO 22000 and other international management standards.
ISP	Internet Service Provider
IVR	An In-Vehicle Router is a device that resides in public safety vehicles, including cars (e.g., police car trunks) or fire apparatus (e.g., trucks) and supports mobile data modems/service connectivity to one or more mobile operators. It can route traffic across different modems in real time, as network coverage and connectivity change.
KPI	A Key Performance Indicator is a measurable value that demonstrates how effectively a telecommunications system is achieving key performance objectives. Most telecommunications systems capture, calculate, and record performance statistics for use in managing the system; a subset of these performance metrics are classified as KPI.
LMR	Land Mobile Radio. A wireless communications system intended for use by users in vehicles (mobiles) or on foot (portables). Such systems are used by emergency/first responder organizations, public works organizations, or companies with large vehicle fleets or numerous field staff.

Term	Definition
LOA	Levels of Assurance are defined by the National Institute of Standards and Technology Special Publication 800-63-2, which details requirements for each of the LOAs in the areas of identity proofing, registration, tokens, management processes, authentication protocols, and related assertions.
Local Control	Local control refers to a collection of capabilities that allow a PSE to influence and control its relationship with the NPSBN.
Local Control Application	A local control application is a specific software application that provides functions for authorized users of a PSE to directly manage elements of its NPSBN environment, including users; devices; roles; profiles; and Quality of Service, priority, and preemption.
Local Control of Business Processes	Local control of business processes refers to ancillary business processes that are part of local control but do not have a computer application to support them (e.g., planned event planning, maintenance window coordination).
Local Control of QPP	Local control of QPP refers to a specific function within the local control application that permits an authorized user to raise or lower the Quality of Service, priority, and preemption (QPP) level of other users within its QPP region.
Local Control QPP Region	Local control QPP region refers to a specific set of cell towers over which an authorized local control user can exercise QPP authority. QPP regions may overlap.
Locked Application	A locked application is a pre-installed or embedded application that is installed on the phone in a manner that prevents the user from deleting or disabling it. Not all pre-installed applications are locked; this often occurs at the request of the carrier when specifying details of the purchase of devices.
LPPa	LTE – Positioning Protocol A
LTE	Long Term Evolution is a standard for wireless communication of high-speed data for mobile phones and data terminals. Commonly marketed as "4G LTE," the standard is developed by the 3GPP (3rd Generation Partnership Project) and is specified in 3GPP's Release 8 document series with enhancements described in later releases.
M2M	Machine-To-Machine , also called the Internet of Things or IoT, is an application-specific set of technologies that allow both wireless and wired systems to communicate with other devices—frequently ones of the same type. Examples of M2M networks include automated meter reading and closed circuit video.
MAM	Mobile application management describes software and services responsible for provisioning and controlling access to internally developed and commercially available mobile apps used in business settings on both company-provided and "bring your own" smartphones and tablet computers.
MBMS	Multimedia Broadcast/Multicast Service is a point-to-multipoint service in which data is transmitted from a single source entity to multiple recipients. Transmitting the same data to multiple recipients allows network resources to be shared. The MBMS bearer service offers two modes: broadcast mode and multicast mode.
MC-PTT	Mission-Critical Push-To-Talk is a standards-based voice capability over LTE defined by 3GPP. As defined by 3GPP, MC-PTT is an enhanced PTT service that includes features such as group, private, broadcast, emergency, and immediate peril calls.
MCS	Modulation and Coding Scheme is used to specify which of the different modulation and coding schemes is being applied.
MCU	--- No longer used in this RFP. Refer to VNS below. ----

Term	Definition
MDM	Mobile Device Management is the administrative area dealing with deploying, securing, monitoring, integrating and managing mobile devices, such as smartphones, tablets and laptops, in the workplace. The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network. See Device Management or DM.

Term	Definition
Middle Class Tax Relief and Job Creation Act of 2012	Pub.L. 112–96, H.R. 3630, 126 Stat. 156, enacted February 22, 2012, with the portions of Title VI related to FirstNet codified at 47 U.S.C. §§ 1401-1457. This Act is FirstNet's enabling legislation. Referred to throughout this RFP as the "Act."
MIL-STD and MIL-STD 810	A United States Military Standard that emphasizes tailoring equipment's environmental design and test limits to the conditions that it will experience throughout its service life. Public safety user devices today nearly always require compliance with MIL-STD durability and environmental guidelines found in MIL-STD-810.
MIMO	Multiple Input, Multiple Output is the use of multiple transmitters and receivers (multiple antennas) on wireless devices for improved performance.
MIS	A Management Information System produces fixed, regularly scheduled reports based on data extracted and summarized from the firm's underlying transaction processing systems for a defined set of users to support and inform structured and semi-structured performance analysis and decision making.
Mission Critical	Any factor of a system (equipment, process, procedure, software, etc.) whose failure will result in the failure of mission operations.
Mission-Critical Infrastructure	Mission-critical infrastructure refers to systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Mission-Critical Services	Mission-critical (MC) services comprises the following services for public safety as they become available in the 3GPP standards: MC-Voice (including MC-Push-to-Talk), MC-Data, and MC-Video and the key support services of enhanced Multimedia Broadcast Multi-cast Services (eMBMS), Group Communication System Enablers (GCSE), and Proximity Services (ProSe).
MLS	The Mobile Location Protocol is an application-level protocol for receiving the position of Mobile Stations (e.g., mobile phones, wireless devices) independent of underlying network technology.
MME	A key node in the EPC, the Mobility Management Entity is responsible for high-level security functions (such as authentication) and manages mobility of the UE while in idle state. It also determines the characteristics of the EPS bearer, based on the requested service and QoS requirements.
MOCN	Multi-Operator Core Network is a network-sharing configuration in 3GPP in which only the RAN is shared.
MRC	Monthly Recurring Charge is a type of billing arrangement whereby the user may consume as much of a service as they wish for a fixed, automatically recurring fee applied to the bill.
MRD	Marketing Requirements Document is an initial specification typically created by a business unit that documents from the users perspective "what" features and functionality is required by the business.
MVNO	A Mobile Virtual Network Operator is a wireless communications services provider that does not own the wireless network infrastructure over which it provides services to its customers. An MVNO enters into a business agreement with a mobile network operator to obtain bulk access to network services at wholesale rates, and then sets retail prices independently. An MVNO may use its own customer service, billing support systems, marketing and sales personnel.
mVPN	A mobile Virtual Private Network is the device resident software that allows the user to establish a secure data session to sensitive data. Similar to the traditional wireline VPN, but for a mobile device.

Term	Definition
Native Code	Native Code refers to an application or service written at the OS level, often in a programming language specific to the OS/Vendor and that may benefit from APIs that are specific to that OS or UE vendor.
NIEF	The National Identity Exchange Federation is a collection of agencies in the United States that have come together to share sensitive law enforcement information. NIEF provides a basic infrastructure consisting of governance, policies and procedures, cryptographic trust, and open standards for securely sharing identity information about users and non-user (system) entities.
NIMS	The National Incident Management System is a proactive approach to guide government departments and agencies, nongovernmental organizations, and the private sector to manage incidents involving all threats and hazards—regardless of cause, size, location, or complexity—in order to reduce loss of life, property and harm to the environment.
NIST	National Institute of Standards and Technology is a non-regulatory agency of the United States Department of Commerce whose mission is innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST standards related to cyber security, software quality, and mobile communications, among others, are employed by FirstNet.
NLETS	National Law Enforcement Telecommunications System is a network for the exchange of law enforcement, criminal justice, and public safety-related information.
NPSBN	FirstNet's mandate, as legislated in the Act, is to ensure the establishment of a Nationwide Public Safety Broadband Network based on a single, national network architecture.
NTIA	National Telecommunications and Information Administration is the Executive Branch agency within the Department of Commerce that is principally responsible for advising the President on telecommunications and information policy issues.
O&M	Operations and Maintenance are the activities that are related to the performance of routine, preventive, predictive, scheduled, and unscheduled actions aimed at preventing equipment failure or decline with the goal of increasing efficiency, reliability, and safety.
OAM	Operations, administration and management or operations, administration and maintenance (OA&M or OAM) is the processes, activities, tools, standards etc. involved with operating, administering, managing and maintaining any system.
OEM	Original Equipment Manufacturer is a term used when one company makes a part or subsystem that is used in another company's end product.
Offeror	Any respondent to this RFP.
OMA	Open Mobile Alliance. A standards body that develops open standards for the mobile phone industry.
OMA-DM	Open Mobile Alliance-Device Management – the specification is designed for management of mobile devices. Device management is intended to support provisioning, device configuration, software upgrades, fault management
OMA-SUPL	Secure User Plane Location is an IP-based protocol for Assisted GPS to receive information of GPS satellites quickly via IP instead of slowly receiving (50 bit/s) over GPS satellite signaling.
OpenID Connect	OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol that allows computing clients to verify the identity of an end user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end user.

Term	Definition
OSS	An Operational Support System is a set of programs that help a communications service provider monitor, control, analyze, and manage a telephone or computer network.
OWASP	The Open Web Application Security Project (OWASP) is an organization focused on improving the security of software and making software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.
PaaS	Platform as a Service refers to the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
PAN	A Personal Area Network is a wireless network established around and connects a single individual's equipment.
PAR	A Performance Assessment Report is used by the COR's to report all minor discrepancies in contractual performance and is sent to the contractor for corrective action, with a copy to the CO.
PBAC	Policy Based Access Controls is a strategy for managing user access to one or more systems, where business classification of users is combined with policies to determine what access privileges a user should have.
PCI	Payment Card Industry
PCRF	Policy and Charging Rules Function is an LTE network element responsible for a) supporting the detection of service data flow, b) the charging system based on this data flow, and c) policy enforcement.
PDN	Packet Data Network. A packet-switched network that can transmit data in digital form, established and operated by a telecommunications administration, or a recognized private operating agency, for the specific purpose of providing data transmission services.
PDP	Policy Decision Point. A server in the Common Open Policy Service (COPS) Protocol, which specifies a simple client/server model for supporting policy control over QoS signaling protocols. Policies are stored on servers, acted upon by Policy Decision Points , and enforced on clients known as Policy Enforcement Points (PEP).
PEP	Policy Enforcement Point. The client server in the COPS that enforces policies on QoS.
Persistent Coverage	Persistent coverage is defined as NPSBN coverage that consistently meets availability objectives without the use of temporary/on-demand coverage solutions.
Persistent Coverage Objective	The persistent coverage objective is the FirstNet baseline, state inputs, and federal inputs as identified in Section J, Attachment J-1, Coverage and Capacity Definitions.
P-GW	PDN Gateway. A key node in the EPC, the P-GW is responsible for anchoring the user plane for mobility between 3GPP access systems and non-3GPP access systems. The P-GW allocates the user's IP address and forwards packets intended for the user to the appropriate Serving Gateway (S-GW). It also provides support for charging, lawful interception, and policy enforcement.
PHI	Personal Health Information is a category of information that refers to an individual's medical records and history, which are protected under the HIPAA.

Term	Definition
PIP	Potentially Interested Party is any interested party to include potential Offerors, end users, Government acquisition and supporting personnel, and others involved, or interested in the conduct or outcome of the acquisition.

Term	Definition
PIV-I	Personal Identity Verification-Interoperable is a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information system in a manner that is interoperable between agencies.
PKI	A public key infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Planned Maintenance	Planned maintenance refers to normal maintenance scheduled for preventative measures (e.g., patches, upgrades) used to deliver stable NPSBN services to end users. This level of maintenance shall occur only after a notice is delivered via electronic communication to and approved by the Government. This requires planning, allocation of significant amount of time and resources, and a high degree of coordination between the Contractor and FirstNet.
PLMN	A Public Land Mobile Network number is a call set-up element that is used to identify a specific mobile operator's network.
PM	Program manager is an individual who manages a range of initiatives to achieve a particular organizational outcome.
POC	Point of contact is a person or a department serving as the coordinator or focal point of information concerning an activity or program.
PRD	Product Requirements Document extends from the MRD by adding additional detail including in-depth functionality, business process follows, and UI wireframes. Different organizations often have different styles of the PRD; there is no universal standard for the format and content of a PRD.
Preemption	A network capability that during an emergency permits authorized high priority traffic, e.g., coming from public safety or first responders, to take over network resources assigned to lower priority traffic, e.g., private traffic.
Pre-Installed Application	Pre-installed application is an application that sits on top of the native OS and is usually encoded in firmware so it survives a hard system boot. The application is pre-installed typically because of convenience or because of partnerships between the carrier and the phone vendor.
Primary User Group	The primary user group consists of law enforcement, fire, and emergency medical services users.
Prime Contractor	A contract award winner that may perform the work alone or with subcontractors.
ProSe	Proximity Services. This mode of communications provides public safety with the ability to communicate UE-to-UE, even when out of range of a wireless network OR when working in a confined area where direct unit-to-unit communications is required.
PS	Public Safety comprises organizations that include, without limitation emergency management agencies, law enforcement agencies, fire departments, rescue squads, and Emergency Medical Services (EMS). Equivalent to PSE.
PSAC	Public Safety Advisory Committee established in February 2013 consists of members representing multiple disciplines of PS as well as state, territorial, tribal, and local governments.
PSAP	A Public Safety Answering Point, sometimes called a Public Safety Access Point, is a call center responsible for answering calls to an emergency telephone number (911) for police, firefighting, and ambulance services.
PSE	Public Safety Entity is defined in Section 6001(26) of the Act as an "entity that provides public safety services." 47.U.S.C. § 1401(26)
PSEN	Public Safety Enterprise Network is a network dedicated to public safety users and their specific requirements and applications.

Term	Definition
PSTN	Public Switched Telephone Network also referred to as plain old telephone service.
PTCRB	Person Communications Services (PCS) Type Certification Review Board. Refer to www.ptcrb.com for an overview of the organization's mission. One of the organization's roles is to certify devices that support LTE for compliance to the applicable 3GPP device related specifications.

Term	Definition
PTT	In an LTE network, Push-To-Talk is a mobile communications technique that emulates two-way radio communications. It is characterized by half-duplex voice whereby the speaker must initiate his or her speech by first pressing a button to gain exclusive ability to speak while other user(s) must listen. Commercial PTT solutions that are not standards-based are available in the market today.
Public Safety Entity Home Page	The Public Safety Entity (PSE) home page is a Web page that can be built, configured, and maintained by an individual PSE. It will contain features such as the status of the network and access to local control information.
Public Safety Grade	The term Public Safety Grade is a conceptual term that refers to the expectation of emergency response providers and practitioners, that their equipment and systems will remain operational during and immediately following a major natural or man-made disaster on a local, regional, and nationwide basis. For the purposes of this RFP, the term is used to refer to network hardening and network sustainability.
Public Safety User	User of the NPSBN that provides public safety services.
QASP	Quality Assurance Surveillance Plan is the key Government-developed surveillance process document that is used to manage contractor performance assessment by ensuring that systematic quality assurance methods are utilized to validate that the contractor's quality control efforts are timely, effective, and are delivering the results specified in the contract or task order.
QCI	QoS Class Identifier defines the general class of the service. There are currently 9 defined. A QCI is associated with a priority, specific delay, and packet loss values, and whether the service has a Guaranteed Bit Rate (GBR). These characteristics will be used by the EPS nodes (eNB, S-GW, P-GW) to guide them in deciding how a particular service data flow is to be processed. The QCI determines such things as resource scheduling, rate shaping, and queue management. At the eNB, the QCI is also used to determine the Radio Link Control (RLC) configuration.
QoS	Quality of Service is the overall performance of a telephony or data network, particularly as seen by the users of the network. To measure quality of service quantitatively, several related aspects of the network service are often considered, such as error rates, bandwidth, throughput, transmission delay, availability, and jitter.
QPP	Quality of service, Priority and Preemption is the back-end network services that must be manipulated by a front-end application that wraps business rules, authentication/authorization, and auditing. See “Local Control of QPP”.
RAN	The Radio Access Network as defined under the Act at 47 U.S.C. 1422(b)(2) as further interpreted by FirstNet’s Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012 [Docket Number: 140821696-4696-01], published October 20, 2015.
RCS	The Rich Communication Services program is a GSM Association (GSMA) program for the creation of inter-operator communication services based on IP Multimedia Subsystem.
Redundancy	Redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system usually in the form of a backup or fail-safe.
Resiliency	Resiliency is the ability to provide and maintain an acceptable level of service in case of infrastructure breakdown or faults to normal operations.
Retainability	Also known as the dropped-call rate, retainability is one of the KPIs used by the network operators to assess the performance of their networks. It has direct influence on customer satisfaction with the service provided by the network and its operator.

Term	Definition
RFI	Requests For Information is a standard business process the purpose of which is to collect written information about the capabilities of various suppliers.

Term	Definition
RFP	Request For Proposal is a solicitation made by an agency or company interested in procurement of a commodity, service, or equipment. As used herein, RFP generally refers to this solicitation for the deployment and operation of the NPSBN as well as use of the FirstNet Band 14 spectrum capacity.
Roaming	Roaming is a technology to ensure a traveling wireless device (typically a cell phone) is kept connected to a network without breaking the connection when leaving the home network geography. When a wireless user travels outside the geographical coverage area of its home network, he or she can still make and receive voice calls, send and receive data, or access other services.
RRC	The Radio Resource Control protocol is responsible for the control plane signaling between the device and the RAN.
RSRP	Reference Signal Receive Power is defined as the linear average over the power contributions (in Watts (W)) of the resource elements that carry cell-specific reference signals within the considered measurement frequency bandwidth. For RSRP determination the cell-specific reference signals R0 and if available R1 according to TS 36.211 [3] shall be used. If the UE can reliably detect that R1 is available it may use R1 in addition to R0 to determine RSRP. If receiver diversity is in use by the UE, the reported value shall be equivalent to the linear average of the power values of all diversity branches.
RSRQ	Reference Signal Received Quality is an indicator of the quality of the received reference signal. It is calculated as (N*RSRP)/(E-UTRA Carrier RSSI), where N ensures the nominator and denominator are measured over the same frequency bandwidth.
Rural	FirstNet defines "rural," for the purposes of the Act, as having the same meaning as "rural area" in Section 601(b)(3) of the Rural Electrification Act of 1936, as amended ("Rural Electrification Act") and as further interpreted by FirstNet's Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012 [Docket Number: 140821696-4696-01], published October 20, 2015.
Rural telecommunications provider	Rural telecommunications provider means an entity that provides either exclusively or the vast majority of its telecommunications or broadband services in a geographic area that falls within the definition of the term "rural" as defined in the Act as interpreted by FirstNet. See First Responder Network Authority, Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012, 80 Fed. Reg. 63523, 29 (October 20, 2015), https://www.gpo.gov/fdsys/pkg/FR-2015-10-20/pdf/2015-26621.pdf.
SaaS	Software as a Service - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.
SAE	System Architecture Evolution is the core network architecture of 3GPP's LTE wireless communication standard. It is the evolution of the General Packet Radio Service (GPRS) Core Network.

Term	Definition
SAFECOM	SAFECOM (Department of Homeland Security) was started after the terrorist attacks of September 11, 2001 to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across federal State, local, tribal, and territorial governments, and international borders.
SAML	Security Assertion Markup Language is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular between an identity provider and a service provider.
SAST	Static Analysis Security Testing refers to technologies and tools that are used for security vulnerabilities in application code, binary, library development before being deployed.
Satellite	A satellite is an orbiting platform used for communications.

Term	Definition
SDK	Software Development Kit. A set of software development tools that allows for the creation of applications for a certain software package, software framework, hardware platform, computer system, operating system, or similar development platform. Typically, an SDK includes one or more APIs, programming tools, and documentation.
SDP	Service Delivery Platform is an architecture platform and business process where the services are created, controlled, monitored for the users to consume for a particular service.
Secondary User	Secondary User is defined under the Act at 47 U.S.C. 1422(b)(1) as further interpreted by FirstNet's Final Interpretations of Parts of the Middle Class Tax Relief and Job Creation Act of 2012 [Docket Number: 140821696-4696-01], published October 20, 2015.
Secure container	Technologies and tools to support enterprise applications and data to be secured at the device and at the servers.
Security Operation Center	A Security Operations Center is a centralized unit that deals with security issues, on an organizational and technical level. An SOC within a building or facility is a central location from where staff supervises the site, using data processing technology. Typically, it is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers.
Service	A service is a form of application that runs in the background of the OS and often does not have a UI. It serves a set of specific functions on behalf of other applications.
Service Capacity	Service capacity refers to when there is sufficient end-to-end network and system resources to meet changing end-user demands for services on the NPSBN, ensuring expected user experience and quality.
S-GW	Serving Gateway is a key node in the EPC, the S-GW acts as an anchor point for the EPS bearer, allowing traffic to flow seamlessly between the UE and the network during inter-eNB handovers.
SICAM	The State Identity and Credential Access Management outlines a strategic vision for state-based identity, credential, and access management efforts in support of the challenges associated with trust, interoperability, security, and process improvement in the state business.
Side-loading	A process of installing an application without using a vendor approved application store. iOS does not support side-loading except for a device that is "jail-broken", configured by the user to bypass vendor installed security. Android does support side-loading without violating vendor established security measures.
SIEM	Security Information and Event Management provides a holistic view of an organization's information technology (IT) security.
SIM	A Subscriber Identity Module is usually a hardware chip that contains encrypted and secure identity and billing information for the mobile network that issues it to the subscriber. Various versions, such as USIM, ISIM, or CSIM, meet the needs of different network technologies and can be placed on one UICC.
SIM Application	An application written on the SIM using the software toolkit.
SIM Application Toolkit	The SIM Application Toolkit consists of a set of commands programmed into the SIM, which define how the SIM should interact directly with the outside world and initiates commands independently of the handset and the network. The software toolkit is essentially a micro programming environment on the SIM that allows the handset vendor to customize various features and execute instructions at an extremely low level of the device.

Term	Definition
SINR	Signal to Interference Plus Noise Ratio is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

Term	Definition
SIP	Session Initiation Protocol is a telecommunications protocol for signaling and controlling multimedia communication sessions.
SLA	Service Level Agreement is an agreement between FirstNet and the Contractor that defines each party's responsibilities, and procedures, needed to ensure that FirstNet's service requirements are met.
Smartphone	A mobile device with more advanced computing capability and connectivity than basic feature phones. The features can typically include personal digital assistant, a media player, a digital camera, GPS navigation touchscreen, web browsing Wi-Fi, 3rd-party apps, and others.
SMC	A Services Management Center is one or more locations from which service and network monitoring and coordinated control and change management is exercised over a telecommunication network or data processing environment. SMC personnel are responsible for monitoring end-to-end services spanning networks for certain conditions, taking necessary actions to avoid degraded service, and communicating and reporting out status. Organizations may operate more than one SMC, either to manage different services and networks, or to provide geographic redundancy in the event of one site becoming unavailable. The SMC encompass the traditional Network Operations Center and includes all aspects of day-to-day operations and management of the end-to-end network.
SOA	A Service-Oriented Architecture is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network. The principles of service-orientation are independent of any vendor, product, or technology.
	[Software Container definition is hereby deleted as a result of Amendment 003]
SON	A self organizing network is a network that can configure itself and manage resources to enable the optimum performance. SON can include self configuration, self optimization, and self healing.
SOO	Statement Of Objectives is a Government-prepared document incorporated into this solicitation that states the overall performance objectives. It is used in solicitations when the Government intends to provide the maximum flexibility to each Offeror to propose an innovative approach to the requested services within the RFP.
SOW	Statement Of Work is a formal document that captures and defines the specific work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client. The SOW usually includes detailed requirements with standard regulatory and governance terms and conditions.
Spectrum	Electromagnetic spectrum refers to the full range of frequencies of electromagnetic radiation. The radio spectrum is the part of the electromagnetic spectrum corresponding to frequencies lower below 300 GHz. The microwave spectrum corresponds to frequencies between 300 MHz (0.3 GHz) and 300 GHz. Band 14, the frequency dedicated to public safety lies within this spectrum.
SSO	Single Sign-On is when a user enters authenticates once and that credential allows the user to access multiple systems, applications, and/or services.
State-deployed RAN	A state-deployed RAN refers to a RAN that a state or territory assumes responsibility for deploying, operating and maintaining in accordance with 47 U.S.C. 1442(e)(2)(B).
Step-up Authentication	Step-up authentication relies on a preconfigured hierarchy of authentication levels and enforces a specific level of authentication according to the policy set on a resource, application, or service.

Term	Definition
Subscriber Adoption	The rate at which new users purchase an appropriate device, subscribe to the network services, and/or begin using network services or capabilities.

Term	Definition
SyncE	Synchronous Ethernet is an ITU-T standard for computer networking that facilitates the transference of clock signals over the Ethernet physical layer.
Systems Integrator	A person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems function together. Systems integrators may work in many fields but the term is generally used in the IT field, the defense industry, or in media.
Temporary Coverage	Temporary coverage is defined as NPSBN coverage not provided by persistent coverage. This type of coverage augments coverage and capacity utilizing on-demand solutions.
Temporary Coverage Objective	The temporary coverage objective has been identified as the area outside of the persistent coverage objective where on-demand solutions are adequate to provide NPSBN coverage.
Territories (U.S.)	These include Puerto Rico, Guam, American Samoa, Northern Mariana Islands, and the Marshall Islands.
The Act	The Middle Class Tax Relief and Job Creation Act of 2012.
Tribal	Of or pertaining to the 566 U.S. federally recognized tribes.
Trustmarks	Trustmarks are the common subset of FirstNet's and a PSE's security policies to allow them to share identity-related information. A common way to describe these security policies has yet to be defined and is an initiative being under taken at a national level within the National Strategy for Trusted Identities in Cyberspace (NSTIC) presidential initiative.
TSP	Telecommunications Service Priority. A system that provides a means for telecommunications users to obtain priority treatment from service providers for the National Security/Emergency Preparedness (NS/EP) telecommunications requirements.
UE	User Equipment is any device or form factor with an LTE radio capable of attaching to the LTE network.
UI	The User Interface of an application is portion of the application the user sees. Commonly in client-server applications, the UI is the tip of the iceberg with significant amount of application code running on the server to support user commands initiated from the UI.
UICC	Universal Integrated Circuit Card is an LTE identity module with one or more unique SIMs with a unique identity that can be tied directly to the billing system.
User	A user refers to a single person who is associated with a public safety agency that uses the NPSBN.
User Group	An arbitrary association of users. User groups are often used in PTT.
User Identifier	A unique ID that identifies a user within the NPSBN and maps to a unique User Profile.
User Profile	A collection of parameters that describe all the attributes of a user. Profiles have some data that rarely or never changes such as birthdays or names as well as data that changes often such as their current status, current role, or what type of device they are using
User Role	Is the current function within the organization or within an incident that a user is currently performing. As with profile data, some roles change little such as a police chief or paramedic and others change often such as incident commander.
VA	A Virtual Assistant sometimes referred to as a Voice Assistant, is a client/server service that translates natural language commands and inquiries into actions (typically across the internet) and provides the requested action or information in a convenient form – often to allow hands-free operation.

Term	Definition
VNS	A Vehicular Network System (previously referred to as a Mobile Communications Unit [MCU]) is a set of radio access and core technologies that enable a first responder's vehicle to act as a virtual cell site for Band 14 users that are out of coverage from the terrestrial network. It is usually equipped with satellite backhaul for remote locations and provides core network features from within the vehicle when the satellite backhaul cannot reach FirstNet's terrestrial core.
VoLTE	Voice over Long Term Evolution. Based on the IP Multimedia Subsystem (IMS) network, voice service (control and media planes) is delivered as data flow within the LTE data bearer, eliminating dependency on the legacy circuit-switched voice network.
VPN	Virtual Private Network extends a private network across a public network, such as the Internet. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.
WEA	Wireless Emergency Alerts is an alerting network in the United States designed to disseminate emergency alerts to mobile devices such as cell phones and pagers.
Web Browser	Web Browser is a native application, typically pre-installed on every phone that can interpret and run HTML scripted applications.
WSP	Wireless Service Provider.

Table of Contents

1 Document Overview

Included below is a sample listing of equipment that may be needed in the FirstNet Test Lab to validate unique public safety features and functions. Offerors shall complete Table 1 Contractor-Furnished Equipment (see Section L, Instructions, Conditions, and Notices to Offerors and Respondents, Section L.3.2.3, Test Strategy) with a specific list of equipment, to be furnished by the Contractor, to enable FirstNet to perform appropriate testing.

Table 1 Contractor-Furnished Equipment

Description of Equipment	Quantity
<example: Three Sector – B14 Indoor Enhanced Node Base station (eNBs)>	<example: 1,000 >
<example: Mobility Management Entity (MME)>	<example: 15>
<example: Serving Gateway (S-GW)>	<example: 1>
<example: Packet Data Network (PDN) Gateway (P-GW) >	<example: 2>
<example: Policy and Charging Rules Function (PCRF)>	<example: 1>
<example: Home Subscriber Server (HSS) >	<example: 1>
<example: Operational Support System (OSS) >	<example: 1>
<example: Business Support System (BSS) >	<example: 1>
<example: IP Multimedia Subsystem or connectivity to one>	<example: 1>

Table of Contents

J Deliverables Table

Table 1 Format of Deliverables Table provides a template and instructions for Offerors to follow when developing their Deliverables Table. The Offeror shall include a Deliverables Table in their response, detailing the deliverables they will provide, including those specified by the First Responder Network Authority (FirstNet) as well as any deliverables that demonstrate the Offeror's technical, business, and management efforts and expertise. Deliverables proposed should align with the performance metrics and standards specified in the Offeror's proposed Quality Assurance Surveillance Plan (QASP) (see Section J, Attachment J-6, Quality Assurance Surveillance Plan, and Section J, Attachment J-9, QASP Surveillance Matrix Template). When developing the Deliverables Table, the Offeror should be attentive to FirstNet's objectives as defined in Section C, Statement of Objectives (SOO).

Table 1 Format of Deliverables Table

Title of Deliverable	Reference	Format	Frequency	Due Date	Associated Performance Metric/ Standard	Relevant SOO Objective(s)
Provide a title for the deliverable.	Reference applicable sections of the Request for Proposal to which the deliverable relates.	Define the format of the deliverable (e.g., report, meeting).	State how often the deliverable will be provided to FirstNet.	Clarify when the first deliverable will be submitted (e.g., contract award, Initial Operational Capability Phase 1).	Note the performance metric/ standard that aligns with the deliverable, as defined in the QASP.	List corresponding objectives from the SOO that the deliverable intends to address.

Table of Contents

1 Delivery Mechanism Objectives for State Plans

The Middle Class Tax Relief and Job Creation Act of 2012 requires the First Responder Network Authority (FirstNet) to deliver a plan to the governor of each of the 56 states and territories notifying the states and territories of the completion of the Request for Proposal process, details of the proposed plan for buildout of the nationwide, interoperable broadband network in said state or territory, and the funding level for the state or territory as determined by the National Telecommunications and Information Administration (the "state plan"). It is FirstNet's intent to present each state plan to each governor via a Web interface developed and hosted by the Contractor.

FirstNet's objectives for the state plan delivery mechanism are as follows:

- Provide the capability for FirstNet, the Contractor, and others to securely upload, edit, delete, search, and display information for a specific state plan.
- Provide access to the information in the State Plan Template (Section J, Attachment J-19) via an easily understood format, using interactive maps, graphics, color-coding, and others as appropriate.
- Include security provisions to manage data access permissions by role to allow for custom views. The solution shall also provide the ability to edit and delete users and roles and the capability to limit individual user access to specific data fields.
- Provide a user-friendly interface that provides for intuitive navigation throughout the full state plan and all of its elements with minimal effort.
- Provide a search function.
- Provide the capability for the user to print selected state plan information.
- Provide documentation accessible from the user interface that lists and explains all included features.
- Provide stable and functional delivery mechanism that is tested thoroughly prior to initial deployment and during system upgrades, enhancements, etc.

Table of Contents

List of Tables

1 Purpose

Text for this section will be provided by the First Responder Network Authority (FirstNet).

2 FirstNet Overview and Mission

Text for this section will be provided by FirstNet.

3 State Consultation

Text for this section will be provided by FirstNet.

3.1 State Governing Body

Text for this section will be provided by FirstNet.

3.2 [State Name] Consultation Process

Text for this section will be provided by FirstNet.

3.3 Outreach and Education Support

Text for this section will be provided by FirstNet.

3.4 State Plan Inputs and Outcomes

Text for this section will be provided by FirstNet.

3.4.1 Minimum Criteria for a State Plan

Text for this section will be provided by FirstNet.

3.4.2 Coverage Objectives

Text for this section will be provided by FirstNet.

3.4.3 User Profiles/Statistics

Text for this section will be provided by FirstNet.

3.4.4 Capacity Planning

Text for this section will be provided by FirstNet.

3.4.5 Current Mobile Data Usage

Text for this section will be provided by FirstNet.

3.5 State Decision Process

Text for this section will be provided by FirstNet.

3.5.1 Summary/Timeline of Actions Required by the State

Text for this section will be provided by FirstNet.

3.5.2 Changes to State Plan Following Decision to Proceed with FirstNet-Deployed Radio Access Network

Text for this section will be provided by FirstNet.

4 State Radio Access Network Plan

Text for this section will be provided by FirstNet.

4.1 Radio Access Network Partner

Identify key network partners and their projected roles within the deployment of the Nationwide Public Safety Broadband Network (NPSBN). Consider including equipment and infrastructure vendors, backhaul services vendors, roaming network partners, network development partners, and state or county partners. Describe any plans to use existing assets, such as existing infrastructure, state, local, tribal, federal land parcels, or other assets.

4.2 Network Design and Key Assumptions

Provide the network planning and design information used for any submissions related to Band 14, including coverage and capacity submissions. Include the following information:

- **Link Curve** – Provide a detailed link curve along with system simulation data showing the relationship between Signal-to-Interference-Plus-Noise Ratio (SINR), code rate, Modulation and Coding Scheme (MCS), and throughput.
- **Planning Tool Settings** – Describe the settings used in the planning tool, including Multiple Input, Multiple Output (MIMO) gains; clutter weights/losses; and environment configurations.
- **Geo-Data** – Provide a detailed description of the geo-data used (e.g., clutter, terrain, clutter height, buildings) including vintage, source, and resolution.
- **Propagation Models** – Provide a detailed description of how the propagation models for planning were generated, noting if they were calibrated or un-calibrated. If calibrated models are utilized, describe how the models were calibrated.

Describe the general design methodologies used to provide indoor and outdoor coverage. Specifically, address the following topics:

- **In-building Strategy Solutions** – Articulate, with metrics, the level of in-building coverage available at each Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestone for Band 14 and any non-Band 14. Within the metrics, include the area covered (in square miles), population covered, and proportion of footprint coverage with useable in-building signal levels. In areas where in-building penetration from the macro network is inadequate, describe

the techniques that will be used to enhance in-building coverage. Identify which in-building solutions will be served with or without Band 14 and include a list of locations for each in-building solution. Take into consideration the size of the in-building location to be covered, expected traffic, and types of services to be supported in the area of interest when selecting the type of in-building systems to be used.

- **Transportation Infrastructure** – Describe the deployment strategy to serve different modes of transportation (e.g., tunnels, railways, ports and waterways, airports, roads). Provide the design, methodologies, sources, and methods used to identify transportation infrastructure coverage requirements and the methodology to determine the appropriate level of indoor, outdoor, and underground service. Provide details on the approach to integration of in-building solutions with the NPSBN.

4.2.1 Coverage Objectives and Requirements

Text for this section will be provided by FirstNet.

4.2.2 RESERVED

[This section was removed in its entirety.]

4.2.3 Link Budget Specifications

Provide the detailed link budget information utilized in the development of the provided coverage maps. The link budget should be provided for all morphologies (dense urban, urban, suburban, and rural) and for each of the 56 states and territories. Within the link budget, include the following information:

- Assumptions, margins, and gains accounted for in downlink and uplink
- Impacts due to various device types
- Maximum allowable path loss, design thresholds, and cell radius

4.2.4 Equipment Performance Specifications

Describe the proposed Radio Access Network (RAN) vendor portfolio, scope of equipment, and feature interoperability to be included with the NPSBN. Provide specifications where applicable and, at a minimum, include the following information:

- A diagram and description of the Long Term Evolution (LTE) base station and sectors, including the antenna system and backhaul components. Identify areas of resource aggregation or redundancy. Describe redundancy mechanisms available in the event a radio fails
- A description of variants of Enhanced Node Base station (eNodeB) platforms available in the current architecture, including specifications for each platform
- Hardware or software techniques utilized to maximize coverage and capacity (e.g., MIMO, carrier aggregation)
- A dimensioning guide for all capacity-dependent hardware and software in the eNodeB. Within the guide, describe the traffic load used in the dimensioning calculation as well as any assumptions made for redundancy
- Solution details if antennae are shared with another frequency band
- The maximum number of radio bearers supported by each variant eNodeB platform

- Details for configurations in which remote radio is involved (e.g., integrated antenna, separate antenna)
- A description of the RAN's congestion management capabilities that would be leveraged in heavy traffic situations
- A description of which of the 16 3GPP-defined Random Access Resource configurations are supported by each eNodeB platform
- A description of all RAN security features

4.2.5 Early Builder Integration

If the proposed solution includes early builder assets, describe the level of effort, strategy, and timelines required to acquire, integrate, and assimilate the early builder equipment and services ("assets") in the respective geographic areas. Describe the early builder assets and how they will be acquired, integrated, and assimilated.

4.2.6 Temporary Coverage Related to Incidents and Planned Events

Describe the strategy for providing temporary incident-level coverage (Band 14 and non-Band 14) and addressing capacity issues using deployable units, satellite, direct mode, or a combination thereof. Describe how temporary coverage and capacity will be provided for areas that are not covered with persistent LTE services. Describe the temporary coverage strategy and solution(s) tailored for each of the individual states and territories.

4.3 State Coverage Summary

Provide descriptions for the state coverage elements listed below.

4.3.1 Persistent Coverage

Submit coverage maps and network statistics, as defined in Table 1 Map Deliverables for Coverage and Capacity and Table 2 Network Statistics Deliverables below, for each of the 56 states and territories to address public safety's needs for coverage and capacity. The coverage maps should depict the cell edge—as defined in Section J, Attachment J-1, Coverage and Capacity Definitions—and service area coverage (i.e., minimum achievable throughput) for the following areas:

- Non-Band 14 Area Coverage
- Non-Band 14 Population Coverage
- Band 14 Network Capacity
- Band 14 Area Coverage
- Band 14 Population Coverage

Table 1 Map Deliverables for Coverage and Capacity

Level	Band	Phase	Number of Maps Required	Format
Nationwide	Non-Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC	Six (6) maps of each file type, depicting coverage by technology: LTE, 3G, 2G, and roaming.	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files
Nationwide	Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC	Six (6) maps of each file type with the LTE analysis layers	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files

Table 2 Network Statistics Deliverables

Coverage Type	Level	Phase
Non-Band 14 Area Covered **	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Non-Band 14 Population Covered	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Band 14 Area Covered	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Band 14 Population Coverage	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC
Band 14 Network Capacity	County	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5, and FOC

** Note: Area coverage statistics should be broken down by technology—LTE, 3G, 2G, and roaming.

Provide the following LTE analysis layers for all Band 14 coverage maps, as noted in Table 1 Map Deliverables for Coverage and Capacity:

- Reference Signal Receive Power (RSRP)
- Best Server
- Downlink SINR
- Uplink SINR
- MCS
- Downlink Average Data Rate
- Uplink Average Data Rate

Provide a composite coverage map with tiered bands to represent areas of expected in-building, in-vehicular, and handheld outdoor coverage.

4.3.2 Coverage Extension Assets for Purchase by Public Safety Entities

Provide a comprehensive list of coverage extension assets, such as a Vehicular Network Systems (VNSs) that will be available to Public Safety Entities (PSEs) for purchase via the customer-facing Web-based portal.

4.3.3 Non-Persistent Cellular Service and Devices

Provide a comprehensive list of non-persistent cellular services, and associated devices, that will be available to a PSE for purchase via the customer-facing Web-based portal. This list may include but is not limited to a VNS with satellite fallback connectivity, a VNS with local eNodeB, Evolved Packet Core (EPC) and applications support, devices that support direct mode (D2D), devices that support Wi-Fi, and devices that support Bluetooth.

4.4 Deployment Phases and Timelines

Provide a schedule noting the timeline for achieving the IOC/FOC milestones for coverage and capacity. Provide a schedule that aligns with the IOC/FOC milestones and describes the planned deployment of coverage by state/territory. Describe roaming networks that may be used in addition to the NPSBN and other networks such as a Mobile Virtual Network Operator (MVNO) network (if applicable).

4.5 Rural Milestones

Text for this section will be provided by FirstNet.

4.6 Network Upgrade and Expansion

The Offeror shall describe the strategy to support necessary network expansion. The strategy shall address coverage, quality, and capacity improvements to the NPSBN and include methodologies and thresholds used to trigger Offeror-defined actions. Improvements may be needed to address the following areas:

- **Coverage** – Extension of coverage to serve new areas (e.g., increase of service area footprint)
- **Capacity** – Additional capabilities to address network congestion (e.g., cell density)
- **Quality** – Improvement of existing capabilities to meet local performance objectives (e.g., strengthening indoor and outdoor coverage)

Provide a framework to facilitate collaboration with local, state, tribal, and federal governments to improve the NPSBN service area and capabilities. Within the framework, address shared or independent efforts to align the NPSBN demand and services. Detail the proposed expansion of in-building coverage via government-owned/supplied equipment.

Describe the strategy, methodologies, and decision thresholds needed to improve:

- **Equipment/System Overlays** – Describe the process for repairing or replacing NPSBN equipment due to feature additions or changes in equipment vendors.
- **Technology Migration** – Describe the process for system-wide migration (e.g., 4G to 5G).

4.7 State Assets

Text for this section will be provided by FirstNet.

4.7.1 Memorandum of Understanding/ Memorandum of Agreement Requirements

Text for this section will be provided by FirstNet.

4.7.2 Tower Sites

Text for this section will be provided by FirstNet.

4.7.3 Backhaul

Text for this section will be provided by FirstNet.

4.7.4 Other State Assets

Text for this section will be provided by FirstNet.

4.8 Spectrum Clearing

Text for this section will be provided by FirstNet.

5 Public Safety Grade

Text for this section will be provided by FirstNet.

5.1 Coverage and Hardening

Describe the network coverage and capacity hardening strategy to be implemented in order to achieve the service availability objectives noted in Section C, Statement of Objectives. Describe plans to exceed local building codes/standards (e.g., deployable strategy, selective site hardening, self-organizing network). Provide a concise summary of the methodology to be employed to ensure that the RAN components, sites structures, radio equipment, and interconnection are designed and implemented to be resilient against failures that can disrupt services to first responders.

5.2 Installation

Provide a schedule noting the timeline for achieving the IOC/FOC milestones for coverage and capacity. Provide a schedule that aligns with the IOC/FOC milestones and describes the planned installation of the NPSBN by state/territory. Describe roaming networks that may be used in addition to the NPSBN and or other existing networks, such as an MVNO network (if applicable).

5.3 Operations and Maintenance

Text for this section will be provided by FirstNet.

5.3.1 Service Availability

Describe the solution to achieve the service availability objectives identified in Section C, Statement of Objectives. Address proposed methods for all layers of the network and associated quality improvement metrics gained as a result of the solution, especially in highly vulnerable key network nodes.

Describe how an integrated service support model that aligns with the Information Technology Infrastructure Library (ITIL®) or commercial equivalent will be delivered. Within the model, include configuration, change, incident, and release management processes.

Describe the National Incident Management System (NIMS) processes and how the processes facilitate communication with the incident commander and emergency operations center (EOC) during localized, regional, or national emergencies or incidents. These processes shall be consistent with Federal Emergency Management Agency guidelines and best practices and include:

- A description of specific support organizations that are stood up in times of localized, regional, or national incidents that must interface, coordinate, and support on-site incident commanders and EOCs
- A plan for reporting and communicating status and performance levels for local, state, tribal, and federal users
- A plan for reporting and communicating impairments and resolution status levels for local, state, tribal, and federal users
- A description of the release management processes in place to introduce features, functionality, and applications into the NPSBN without impacting user services
- A description of the business continuity management processes in place, including provisions of disaster recovery and major event support to local, state, tribal, and federal agencies

- A description of the ongoing service-level management processes that provide a continued baseline of system and per service performance, including proactive improvement plans for increased performance, service, and support of NPSBN users
- A description of the availability management processes in place, including ongoing analysis of availability failures, contingency planning, and other activities and processes to ensure service availability objectives are met
- A description of the capacity management processes in place to meet current and future NPSBN objectives. Include descriptions of how NPSBN utilizations, including computing, storage, network, and application sizing, will be managed to ensure ongoing service levels
- A description of the national and local support structure to provide on-site support for both reactive and proactive configuration, maintenance, and monitoring activities. Include network optimization activities and quality assurance activities for the NPSBN
- A description of the protocols and processes to address state and local support of natural disasters and major events requiring deployable assets. Include quantities of deployable assets and the default distribution of assets to support rapid response; procedures to request assets (both proactively and reactively); and a description of deployment, operations, and support during such events.

5.3.2 Customer Care and Support

Describe the proposed customer care strategy, including how the strategy minimizes churn and promotes customer retention among public safety users. Describe how an integrated customer care model will be delivered for public safety users. Provide a description of the customer care organization(s) that will support the NPSBN, including the organization's function, size, structure, geographic distribution (e.g., whether resources are based in the United States; the location and number of employees/subcontractors located outside of the United States), and relation to the Offeror (i.e., in-house, contracted out). Describe the proposed solution for resolving customer service requests or issues with service delivery or products, including how the Contractor will provide responsive corrective actions for service impairments and service restoral when corrective action involves direct contact with the customer. Describe training the customer will be provided for devices and services. Describe the proposed strategies for recruitment and retention of the customer care workforce, including how to train staff on existing and emerging products, services, and applications. Additionally, describe any customer care systems and tools that will be used in support of public safety customer care.

5.3.3 Services Management Center

Provide a clear, concise description that demonstrates how the Services Management Center (SMC) is structured. Include the following details:

- Describe the SMC location(s) and structure(s) that support the various network and service support functions, including applications, billing and provisioning, content services, devices, network (Core, RAN, Wide Area Network [WAN]), security, surveillance, and service desk.
- Describe the technical support staff and resources available among each network and service function and how service troubleshooting is orchestrated by the SMC for varying levels of service. Detail how the SMC is made aware of all on-call staff spanning local/on-site locations to Core/national locations.
- Describe the process of how public safety users originate a request or service issue into the SMC and how staff correlate and assess if a larger issue affecting users exists.

- Describe the network and element management systems that provide real-time monitoring and dashboards of the end-to-end network. Detail how individual alarms are rolled up and correlated to service-based events. Include how SMC staff members are effectively prepared to respond, resolve, or route events to the appropriate next tier of support.
- Detail how incidents are effectively managed and communicated based on the severity and location. Describe how an incident life cycle is managed and effectively handed off between SMC shifts. Describe how states and agencies can access and understand incident information in real time.
- Describe the management and Key Performance Indicators (KPIs) around messaging of service status as well as its effectiveness in the identification and resolution of service degradation issues.
- Training plan for all SMC staff.
- Continuity staffing plan for key SMC positions.

5.3.4 Status Reporting to States and Territories

Describe the mechanisms that will be used to report the status of the NPSBN to each of the 56 states and territories. A sampling of potential reports that Contractor may make available is listed below.

- Deployment Status Report
- Planned Maintenance Report
- Planned Upgrade Report
- Customer Care Summary Report
- Customer Service Issue Resolution Report
- Network Performance
- Key performance indicators regarding coverage and capacity
- Hardware and Software Change Management Report
- Service Availability Report
- Business Continuity Testing Report
- Disaster Recovery After-Action Report
- Hardware and Software (Past and Future) Release Management Report

5.3.5 Public Safety Enterprise Network/Public Safety Answering Point Integration

Describe the approach to integrating Public Safety Enterprise Networks (PSENs) and Public Safety Answering Point (PSAPs) with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). Provide the details of the solution to grow, manage, maintain, and report on PSEN and PSAP connections, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments and removals. This should include an architecture, design, maintenance, and management plan that aligns with the IOC/FOC milestones and continues after FOC. Within the plan, include the following information:

- Integration and testing schedule
- Integration test plan
- Integration performance report
- Risk and jeopardy mitigation report
- Integration and testing completion report
- Roadmap

Describe how the status of actual and planned PSEN and PSAP integration will be reported to the state or territory.

5.4 Network Reliability

Describe the strategy for addressing network reliability and maximizing availability of all network elements.

5.5 Network Resiliency

Provide the network design including survivability assumptions to maintain an acceptable level of service in the face of natural disasters, faults and other challenges, which may include but are not limited to any natural or man-made events that adversely impact Public Safety Entities' access to or use of the NSPBN pertaining to normal operation. Outline the process to maintain and improve network resiliency for the NPSBN.

5.6 Network Redundancy

Provide the design and redundancy detailed needed to achieve the service availability objectives. This may be accomplished through local and geo-redundancy for all NPSBN components, systems, and links or via other means. This should cover proposed methods for all layers of the network and any associated quality improvement metrics gained as a result of these solutions especially in highly vulnerable key network nodes. Include strategies that, at a minimum, address the following:

- **Backup Power** –Provide, on a per state basis, the percentage and location of sites to be configured with the backup power systems, the types of backup systems, and the average runtime between service and refueling. Include detail plans about portable generators.
- **Resilient Interconnection** –Provide, on a per state basis, the percentage of site infrastructures hardened against backhaul failure with multiple independent interconnections capable of individually handling the expected traffic from the wireless facilities.

5.7 Environmental Factors

Document and provide specific actions being taken in the design and implementation of the NPSBN to mitigate environmental factors that could have an adverse effect on the NPSBN performance. Document and provide the solutions for different regions impacted based on specific environmental factors relevant for each of the 56 states and territories. Include a weatherization strategy of how cell sites located in areas prone to specific adverse weather conditions are addressed. This shall include but is not limited to flooding, storm surges, tornados, earthquakes, hurricanes, ice storms, and wild fires.

5.8 Security

Text for this section will be provided by FirstNet.

5.8.1 Security Architecture Plan

The Contractor shall provide a complete functional and physical depiction of the security layout of the NPSBN across and within each of the respective security subdomains including RAN, Core, User

Equipment (UE), Application, and backhaul. This architectural plan will include at a minimum specifications and methods for ensuring security for each of the respective security subdomains and the interfaces both internal and internal affecting each.

5.8.2 Security Integration and Test Plan

The Contractor shall deliver a written plan that covers, at a minimum, the methods and approach to onboarding updates, hardware, operating systems, LTE updates, and related systems and with associated testing to ensure optimal functionality within the approved security architecture. This document should also provide mitigation strategies for required updates that potentially introduce operational impacts.

5.8.3 Applications Security Plan

The Contractor shall deliver a formal plan detailing the means, methods, and strategy for securing the application ecosystem and the inherent functions of application creation, delivery, updating, and validation. At a minimum, this will also include validation of authorized access to the application ecosystem and protection of data in transit from/to applications to external databases and on the local device data storage.

5.8.4 Security Monitoring Plan

The Contractor shall provide a plan that details the methods and techniques to conduct security monitoring across the FirstNet environment. At a minimum, this plan will include technologies employed, reports provided, a logging approach and related forensic analysis of those logs, and incident response capability and timeliness, as well as a mitigation process and related escalation/de-escalation notification processes and criteria.

5.8.5 Security Configuration Management Plan

The Contractor shall conduct tracking, planning, development, and implementation of new Computer Network Defense/Cybersecurity capabilities into all FirstNet NPSBN systems. The contractor shall provide documented methods, techniques, processes in a written plan to ensure configurations of device level, network, applications, and related components are known and changes captured prior to implementation.

5.8.6 Technical Analysis and Security Review of Security Tools

The contractor shall provide technical and management support to FirstNet in planning, development and testing of security technologies; provide technical analysis in support of development and test activities for new systems and emerging technologies; facilitate development of future requirements and architectures that enable transition of new systems and technologies into the operational baseline. The contractor shall provide the methods, processes, and procedures to document suitability, security validation and integration activities.

5.8.7 Physical Security Plan

The Contractor shall provide FirstNet with a documented plan covering the processes, procedures, and technologies to provide for the physical security and physical monitoring of sites of the FirstNet NPSBN. The plan will include but is not limited to intrusion monitoring (facility and cabinets/racks), power and power levels, water and humidity monitoring, access controls and heating/cooling.

5.8.8 Cybersecurity Incident Response Plan

The Contractor shall provide FirstNet with a documented Cyber Incident Response Plan that includes but is not limited to computer security monitoring to rapidly detect incidents, vulnerability detection and analysis, log collection and analysis, tracking and reporting of incidents and restoration of IT operations after an incident occurs. The plan shall include specific technical processes, techniques, checklists, and forms to be used by the incident response teams. The Contractor shall document methods to report and escalate incidents to FirstNet in a timely fashion.

6 Network Operator/User Training Requirements

Provide a training plan describing the level of assistance provided to First Responders to utilize the full capabilities of the NPSBN and MVNO. This assistance may include training on equipment, features, and services available for normal and emergency operations.

7 State Decision Process/Requirements/Timeline

Text for this section will be provided by FirstNet.

7.1 Proceeding with FirstNet-Deployed RAN – Next Steps and Process to Submit Questions

Text for this section will be provided by FirstNet.

7.2 Consultation Roles and Responsibilities after the Plan is Accepted

Text for this section will be provided by FirstNet.

7.3 Decision to Proceed with State-Deployed RAN – Procedures

Text for this section will be provided by FirstNet.

7.3.1 Decision to Proceed with State-Deployed RAN Plan Requirements

Text for this section will be provided by FirstNet.

7.3.2 Decision to Proceed with State-Deployed RAN Plan Criteria

Text for this section will be provided by FirstNet.

7.3.3 Decision to Proceed with State-Deployed RAN Plan Submission Process

Text for this section will be provided by FirstNet.

7.4 Timeline

Text for this section will be provided by FirstNet.

APPENDIX A FirstNet Nationwide Design

Text for this section will be provided by FirstNet.

A.1 End-to-End Network Architecture

Describe and document the NPSBN end-to-end architecture solution—RAN, EPC, infrastructure, services, application platforms, and OSS/BSS—that is dedicated for public safety users. The solution shall be capable of integrating with existing non-Band 14 RAN, where applicable as well as with state deployed RANs.

Provide evidence in achieving the quality metrics noting past performance or that of partners.

Include in the NPSBN end-to-end architecture:

- Architecture descriptions and diagrams including physical, logical and geographic architectures
- High Level Design criteria, objectives and components utilized
- Software releases and 3GPP standards implemented
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions
- Design criteria and objectives utilized for each of the 56 states and territories, in separate documents, to maximize system availability, resilience, and reliability.

A.1.1 State RAN Architecture

The RAN strategy and solutions shall encompass the architecture, design, and deployment strategies that effectively use resources, skillsets, organizational structure, and tools. Demonstrate the following capabilities with respect to RAN solutions and potentially include a combination of maps and tables showing relevant statistics and brief descriptions of features and services.

Provide a reference list of air interface standards and/or non-standard interfaces to be implemented in the proposed network for communication between the eNodeB and User Equipment. These shall comport with those outlined in Section J, Attachment J-4, System and Standard Views. The description for the RAN architecture should include:

- Architecture descriptions and diagrams including physical, logical, and geographic architectures.
- High Level Design criteria, objectives and components utilized
- Software releases and 3GPP standards implemented
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions
- Design criteria and objectives utilized for each of the 56 states and territories, in separate documents, to maximize system availability, resilience, and reliability.

A.1.2 Nationwide Core Architecture

Describe and document a Core network solution—EPC, services, application platforms, and OSS/BSS—that is dedicated for public safety users. The solution shall be capable of integrating with FirstNet NPSBN RANs (Band 14 and Offerors' bands) as well as state-deployed RANs.

The description of the NPSBN Core network should include:

- Architecture descriptions and diagrams including physical, logical and geographic architectures
- High Level Design criteria, objectives and components utilized
- Software releases and 3GPP standards implemented
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions
- Design criteria and objectives utilized for each of the 56 states and territories, in separate documents, to maximize system availability, resilience, and reliability.

A.1.3 Backhaul, Aggregation, Transport, and National Transmission Network Architecture

Describe and document a transmission network solution— backhaul, aggregation, transport and national transmission network. The descriptions of the NPSBN backhaul, aggregation, transport and national transmission network should include:

- Architecture descriptions and diagrams including physical, logical and geographic architectures
- High Level Design criteria, objectives and components utilized
- Software releases and 3GPP standards implemented
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions
- Design criteria and objectives utilized for each of the 56 states and territories, in separate documents, to maximize system availability, resilience, and reliability.
- A roadmap according to IOC/ FOC target milestones for the transmission systems strategy

A.1.4 Operational Support System Architecture

Describe and document an OSS solution—EMS, NMS, workflow, change management, trouble ticketing, troubleshooting support and diagnostic platforms that are utilized for the NPSBN. Provide a description of the NPSBN OSSs and include:

- Architecture descriptions and diagrams including physical, logical and geographic architectures
- High Level Design criteria, objectives and components utilized
- Software releases and 3GPP standards implemented where applicable
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions
- Design criteria and objectives utilized to maximize system availability, resilience, and reliability.

A.1.5 Business Support System Architecture

Describe and document a BSS solution—Customer Relationship Management (CRM), billing, accounting/finance, asset management, logistics management, customer trouble ticketing, customer trouble shooting support and diagnostic platforms that are utilized for the NPSBN. Provide a description of the NPSBN BSSs and include:

- Architecture descriptions and diagrams including physical, logical and geographic architectures
- High Level Design criteria, objectives and components utilized
- Software releases
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions
- Design criteria and objectives utilized to maximize system availability, resilience, and reliability.

A.1.6 Applications Architecture

Provide the architecture for the NPSBN Applications, which includes the service delivery platform, application development platform, hosting and cloud services, application store, application life cycle management, application certification and security. The description of the applications architecture should include, but not be limited to:

- Overall architecture with descriptions and diagrams
- High Level Design criteria and objectives/capabilities
- Application development environment
- Application APIs and SDKs
- External interfaces and specific dependencies to include but not limited to the following: cloud services, Core components, devices and database access

A.1.7 Interconnection Architecture

Provide the interconnection and interworking architecture supporting state-deployed RAN backhaul aggregation integration, PSEN and PSAP integration, PSTN integration, PLMN integration, and roaming to the Core systems across all integrated networks (MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network implementation and operation. Describe the interconnect and interworking architecture nothing how it will be maintained and managed and how the state will be informed as to its status. Provide a roadmap according to IOC/ FOC target milestones for their interconnection and interworking strategy.

The description of the NPSBN interconnection architecture should include:

- Architecture descriptions and diagrams including physical, logical and geographic architectures
- High-level design criteria and objectives and components utilized
- Software releases
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/ FOC target milestones including components, functionalities and design criteria evolutions

- Design criteria and objectives utilized to maximize system availability, resilience, and reliability

A.2 End-to-End Network Design (Logical and Physical)

Describe and document the NPSBN end-to-end detailed design solution—RAN, EPC, infrastructure, services, application platforms, and OSS/BSS.

The description of the NPSBN end-to-end design should include:

- Detailed descriptions and diagrams including physical, logical and geographic designs for all components, links and systems
- Detailed design criteria and objectives for each component utilized
- Software releases implementation schedules and 3GPP standards implemented
- External interface detailed designs and connections guidelines
- Detailed Design criteria and objectives utilized for each of the 56 states and territories, in separate documents, to maximize system availability, resilience, and reliability.

Include the operational process, metrics, and thresholds associated with:

- Failure restoration
- Degradation restoration
- All upgrade(s)/update(s) including 3GPP upgrade process to ensure timely deployment of public safety services that are being standardized in the future.
- Deployment risk mitigation
- Capacity and traffic growth performance
- Capacity and traffic growth exhaust
- Roaming performance between Band 14 and other networks
- Network restoration for disaster recovery and reaction to major incident

A.2.1 Radio Access Network Design

Describe and document the NPSBN RAN detailed design solution. The description of the NPSBN RAN detailed design should include:

- Detailed descriptions and diagrams including physical, logical and geographic designs for all components, links and systems
- Detailed design criteria and objectives for each component utilized
- Software releases implementation schedules and 3GPP standards implemented
- External interface detailed designs and connections guidelines
- Detailed Design criteria and objectives utilized for each of the 56 states and territories, in separate documents, to maximize system availability, resilience, and reliability.

Include the operational process, metrics, and thresholds associated with:

- Failure restoration
- Degradation restoration
- All upgrade(s)/update(s) including 3GPP upgrade process to ensure timely deployment of public safety services that are being standardized in the future

- Deployment risk mitigation
- Capacity and traffic growth performance
- Capacity and traffic growth exhaust
- Roaming performance between Band 14 and other networks
- Network restoration for disaster recovery and reaction to major incident

A.2.2 Core Design

Describe and document the NPSBN Core detailed design solution. The description of the NPSBN Core detailed design should include:

- Detailed descriptions and diagrams including physical, logical and geographic designs for all components, links and systems
- Detailed design criteria and objectives for each component utilized
- Software releases implementation schedules and 3GPP standards implemented
- External interface detailed designs and connections guidelines
- Detailed design criteria and objectives to maximize system availability, resilience, and reliability.

Include the operational process, metrics, and thresholds associated with:

- Failure restoration
- Degradation restoration
- All upgrade(s)/update(s) including 3GPP upgrade process to ensure timely deployment of public safety services that are being standardized in the future
- Deployment risk mitigation
- Capacity and traffic growth performance
- Capacity and traffic growth exhaust
- Roaming performance between Band 14 and other networks
- Network restoration for disaster recovery and reaction to major incident

A.2.3 Backhaul and Transport Design

Provide the transmission systems detailed design plan supporting RAN backhaul, backhaul aggregation, a nationwide backbone transmission system and associated transmission security, routing methodologies and service prioritization including end-to-end Quality of Service and priority integrity across LTE and transport layers.

Descriptions of the Transmission systems should include a detailed design, maintenance and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- Transmission systems traffic, capacity and growth plan
- Detailed network designs
- Description of reports that the state will receive which may include
    - Upgrades and update report
    - Configuration change report
    - Provisioning report (assignments, builds and removals)
    - Transmission network and link bandwidth utilization reports

- Transmission network and link SLA Report (availability, outage, etc.)

A.2.4 Operational Support System Design

Describe and document the NPSBN OSS detailed design solution. The description of the NPSBN OSS detailed design should include:

- Detailed descriptions and diagrams including physical, logical and geographic designs for all components, links and systems
- Detailed design criteria and objectives for each component utilized
- Software releases implementation schedules
- External interface detailed designs and connections guidelines
- Detailed design criteria and objectives to maximize system availability, resilience, and reliability

Include the operational process, metrics, and thresholds associated with:

- Failure restoration
- Degradation restoration
- All upgrade(s)/update(s)
- Deployment risk mitigation
- Capacity and traffic growth performance
- Capacity and traffic growth exhaust
- OSS restoration systems for disaster recovery and reaction to major incident

A.2.5 Business Support System Design

Describe and document the NPSBN BSS detailed design solution. The description of the NPSBN BSS detailed design should include:

- Detailed descriptions and diagrams including physical, logical and geographic designs for all components, links and systems
- Detailed design criteria and objectives for each component utilized
- Software releases implementation schedules
- External interface detailed designs and connections guidelines
- Detailed design criteria and objectives utilized to maximize system availability, resilience, and reliability

Include the operational process, metrics, and thresholds associated with:

- Failure restoration
- Degradation restoration
- All upgrade(s)/update(s)
- Deployment risk mitigation
- Capacity and traffic growth performance
- Capacity and traffic growth exhaust
- Network restoration for disaster recovery and reaction to major incident

A.2.6 Applications and Services Design

The Offeror shall provide a description of the architecture for the NPSBN applications ecosystem, which includes the service delivery platform, application development platform, hosting and cloud services, application store, application life cycle management, application certification and security. The description of the applications ecosystem should include, minimally, the following:

- Overall architecture with descriptions and diagrams
- High Level Design criteria and objectives/capabilities
- Application development environment
- Application APIs and SDKs

External interfaces and specific dependencies to include but not limited to the following: cloud services, Core components, devices, and database access.

A.2.7 Interconnection Design

Provide an interconnection and interworking approach and plan supporting state deployed RAN backhaul aggregation integration, PSEN and PSAP integration, PSTN integration, and PLMN integration to the Core systems across all integrated networks (e.g. MVNO, Core, Roaming partners, and state deployed RANs) to form a seamless network implementation and operation. Provide an ongoing interconnect and interworking plan to grow, maintain, manage, and report on these connected systems including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. Provide a roadmap according to IOC/ FOC milestones for their interconnection and interworking strategy.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- Interconnection, interworking and test schedule
- Interconnection and interworking test plan
- Description of reports that the state will receive which may include
    - Interconnection and interworking performance report
    - Risk and jeopardy mitigation report
    - Interconnection, interworking and test completion report

A.3 Products and Services

Provide the products and services roadmaps. Roadmaps should be provided for network technology, network services, public safety specific products and services and any other applicable technology standards and releases, vendor equipment capabilities, features, and services identified for inclusion into the NPSBN and how it specifically addresses public safety needs. The roadmap shall include the target availability date for each item described. Identify the 3GPP release supported. Provide hardware, software/feature evolution roadmap, and insight into impacts to the NPSBN.

A.3.1 Products Roadmap

Provide the products roadmaps. Roadmaps should be provided for network technology, public safety specific products and any other applicable technology standards and releases, vendor equipment capabilities identified for inclusion into the NPSBN and how it specifically addresses public safety needs. The roadmap shall include the target availability date for each item described. Identify the 3GPP release supported. Provide product hardware, software/feature evolution roadmap, and insight into impacts to the NPSBN.

A.3.2 Services Roadmap

Provide the services roadmaps. Roadmaps should be provided for network services, public safety specific services and any other applicable service standards and releases, features, and services identified for inclusion into the NPSBN and how it specifically addresses public safety needs. The roadmap shall include the target availability date for each item described. Identify the 3GPP release supported and provide each service evolution roadmap and insight into impacts to the NPSBN.

A.4 Nationwide Core Network

Text for this section will be provided by FirstNet.

A.4.1 Roaming Strategy

Document and provide the overall NPSBN roaming solution design and strategy for roaming partners. The design solution should include roaming between NPSBN and partner networks as well as other wireless systems (i.e., Wi-Fi) while maintaining session continuity and appropriate QPP parameters. The solution should explain the approach to use roaming partners to comply with coverage requirements. Provide a roadmap according to IOC/ FOC target milestones for roaming strategy milestones.

A.4.2 Roaming Partner Integration

Provide a roaming partner integration plan. The plan should include the solution for roaming between Band 14 and roaming partner's Band 14 and non-Band 14 systems while maintaining session continuity and appropriate QPP parameters. Include the roaming partner architecture, high-level design and detailed designs as well as an integration plan and schedule.

A.4.3 Network Specifications

Provide detailed network specifications, design criteria, and operational metrics of the solution to the following:

- All Application platforms, enabling systems such as IMS, EPC systems, transmission systems, OSS and BSS Interface
- Detailed specifications of any non-standard or specialized equipment
- Detailed specification of all external network interconnection points such as PSTN, PSENs, ISPs, WSPs, etc.
- All NPSBN, OSS and BSS Quality

- RAN/Core integration including the O&M interfaces between RAN and Core in support of NPSBN operations center

A.4.4 Session Continuity

Document the solution to ensuring session continuity between NPSBN and other networks for the following:

- Voice, data and streaming sessions
- Signaling sessions

The description should detail how the solution will achieve service continuity for each IOC and FOC milestone.

A.5 Logical Architecture (System Views for User and Control Plane)

Provide a logical architecture document that includes system views for all user and control planes for all, but not limited to, the following platforms, systems, and components:

- All network and service platforms including SDP, IMS, EPC systems, transmission systems, location systems, presence systems and security systems
- All BSS including billing, provisioning, asset management, CRM, and financial systems
- All OSS systems including Network Management Systems (NMS), Element Management systems, trouble ticketing systems, change management systems, planned work/workflow systems
- All end-to-end security systems including firewalls, IDS, Security Gateway, border control, monitoring, resolution and investigation systems

A.5.1 Covered Leasing Agreement User Integration

Provide a solution and plan to integrate CLA users including:

- Overall CLA user integration methodology and design
- Ensuring no adverse impact to public safety users under normal operating conditions as well as challenging conditions (natural or man-made)
- Proposed quality metrics applicable to CLA users

A.5.2 Compliance to 3GPP Standards MVNO Strategy

If the solution includes an MVNO implementation, include the following:

- The schedule of MVNO service availability to Public Safety
- The proposed capabilities to be offered under the MVNO
- A migration plan from MVNO to NPSBN
- The quality specification and user performance of services and functionality of the MVNO network
- The methodology of interworking between NPSBN and MVNO including key considerations, parameters and quality metrics

- A roadmap according to IOC/ FOC target milestones for the MVNO strategy milestones.

A.5.3 Key Core Network Locations

Provide information about the key core network locations utilized in the NPSBN.

- Layout and configuration of all key core network locations such as datacenters, switching, routing and transmission hubs
- Core location Infrastructure (mechanicals, fire suppression, racks, cabinets, primary, power, back-up power, HVAC)
- Core location TIA 942 Classification
- Core location type (owned or leased space, leased rack, etc.)
- Physical security access and egress policies
- Entrance facility redundancy and spatial diversity (Power, Transmission, etc.)
- Geographic Zoning Classification

A.5.4 Radio Access Network Backhaul Architecture and Topology

Provide RAN backhaul architecture, topology and synchronization approach across integrated networks (e.g., MVNO, Core, Roaming partners, and state deployed RANs) to form a seamless network implementation and operation. Outline the plan to maintain and manage RAN backhaul architecture, topology and synchronization systems and components including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- RAN backhaul and synchronization traffic, capacity and growth plan
- RAN backhaul and synchronization architecture and topology designs
- RAN backhaul and synchronization detailed network designs
- Description of reports that the state will receive, which may include:
    - RAN backhaul and synchronization upgrades and update report
    - RAN backhaul and synchronization configuration change report
    - Provisioning report (assignments, builds and removals)
    - RAN backhaul and synchronization link bandwidth utilization reports
    - RAN backhaul and synchronization link SLA Report (availability, outage, etc.)
- A roadmap according to IOC/ FOC target milestones for the RAN backhaul architecture, topology, and synchronization strategy.

A.5.5 Radio Access Network Backhaul Aggregation Transport Network

Provide architecture and design of the RAN backhaul system aggregation transport network approach across integrated networks (e.g., MVNO, Core, Roaming partners, and state deployed RANs) to form a seamless network implementation and operation.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- RAN backhaul system aggregation traffic, capacity and growth plan
- RAN backhaul system aggregation architecture designs
- RAN backhaul system aggregation detailed network designs
- Description of reports that the state will receive, which may include
    - AN backhaul system aggregation upgrades and update report
    - RAN backhaul system aggregation configuration change report
    - RAN backhaul system aggregation provisioning report (assignments, builds and removals)
    - RAN backhaul system aggregation bandwidth utilization reports
    - RAN backhaul system aggregation SLA Report (availability, outage, etc.)
- A roadmap according to IOC/ FOC target milestones for the RAN backhaul system aggregation transport network strategy

A.5.6 National Transmission Network

Provide architecture and design documentation of its national transmission network approach across integrated networks (e.g., MVNO, Core, Roaming partners, and state deployed RANs) to form a seamless network implementation and operation.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- National transmission network traffic, capacity and growth plan
- National transmission network architecture designs
- National transmission network detailed network designs
- Description of reports that the state will receive, which may include:
    - National transmission network upgrades and update report
    - National transmission network configuration change report
    - National transmission network provisioning report (assignments, builds and removals)
    - National transmission network and link bandwidth utilization reports
    - National transmission network and link SLA Report (availability, outage, etc.)
- A roadmap according to IOC/ FOC target milestones for the national transmission network strategy.

A.5.7 Transport Security

Provide architecture and design documentation of the transport security approach across integrated networks (e.g. MVNO, Core, Roaming partners, and state deployed RANs) to form a seamless network implementation and operation.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- Transport security traffic, capacity and growth plan
- Transport security architecture designs
- Transport security detailed network designs
- Description of reports that the state will receive, which may include:

  - Transport security upgrades and update report
  - Transport security configuration change report
  - Transport security provisioning report (assignments, builds and removals)
  - Transport security SLA Report (availability, outage, etc.)
- A roadmap according to IOC/ FOC target milestones for the transport security systems and components strategy.

A.5.8 Routing and DRA strategy

Provide architecture and design documentation of its diameter signaling approach across integrated networks (e.g., MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network implementation and operation.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC, including but not limited to the following:

- Routing and DRA traffic, capacity and growth plan
- Routing and DRA architecture designs
- Routing and DRA detailed network designs
- Description of reports that the state will receive, which may include:
  - Routing and DRA upgrades and update report
  - Routing and DRA configuration change report
  - Routing and DRA provisioning report (assignments, builds and removals)
  - Routing and DRA SLA Report (availability, outage, etc.)
- A roadmap according to IOC/ FOC target milestones for routing and DRA strategy.

A.5.9 Transport Service Prioritization

Provide architecture and design documentation of its transport service prioritization approach across integrated networks (e.g., MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network implementation and operation. Provide an ongoing transport service prioritization plan to grow, maintain, manage, and report on the transport service prioritization including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. Provide a roadmap according to IOC/ FOC target milestones for the transport service prioritization strategy.

A.6 Network Services

Provide a description of the design for each network service the following:

- High-level design (include logical architecture, physical architecture, redundancy, overload, call flows, data flows and message flows, interface design for both internal and external component, network and system design, design parameters, components and network systems impacted to enable or support the service)
- Detailed service design specifications (includes items such as specific parameters or service enablers that will be implemented to support the service (e.g. GCSE for MCPTT), specific routing and failover to ensure service SLAs and any component, network or system changes required to implement the service)

- Implementation Plan (Includes project milestones for implementation of key systems and components to support the services, configuration guide, as-built documentation, end to end testing to verify service continuity and acceptance into operations as an operational service).
- Define and provide KPIs and SLAs for each service as well as KPI and SLA service improvement plans.
- Provide a description of the reports that the state will receive noting frequency and performance data to be included for each service
- Provide a description of the service data sources and statistics that will be provided to the state for all service KPIs and SLAs noting the format to display.

A.6.1 Basic Services

Provide the design of the basic network services solution based on the current commercial service offerings to provide public safety users basic communications services. The description of the basic network services for the NPSBN should include the following services:

- **Messaging** – Describe the support for text messaging, MMS, instant messaging, email, voice mail, chat, and Rich Communications Services (RCS)
- **Streaming Video/Audio Services** – Describe how the solution will incorporate video services, and make those services and feeds available to users and applications
- **Voice telephony (VoLTE, VoIP, circuit switched, etc.)** – Describe how the solution will support voice communications throughout the footprint in cellular, Wi-Fi, and their interworking with IP PBX/PSTN
- **Machine to Machine** – Describe the design of device to device/ machine communications and data exchange within the NPSBN as well as to and from external networks
- **IMS Services** – Describe the design of the proposed architectural framework to deliver multimedia services, with the focus on how to interoperate with another carrier's IMS and also third-party IMS application providers
- **Broadcast and Multicast Services** – Describe the design of the proposed broadcast and multicast services for bandwidth intensive communications
- **Presence** – Describe the design of the proposed Presence and discovery services
- **Location** – Describe the design of the proposed Location based services with accuracy for x, y coordinates
- **Device Management** – Describe the design of the proposed device configurations, accounting and logging, authentication, encryption, key management, lockdown, and status tracking
- **Device Authentication** – Describe the design of the proposed mutual device-network authentication, encryption, and integrity protection
- **Lawful Intercept** – Describe the design of CALEA to intercept both signaling and bearer information for specific users
- **NG911 Services** – Describe the design of interconnecting and sending information to PSAPs
- **Wireless Emergency Alerts (WEA)** – Describe the design of WEA

A.6.2 Mission Critical Services

Describe the roadmap, high-level design, and product development timing, in accordance with the target milestones outlined in Section J, Attachment 8, IOC/FOC Target Milestones, for mission critical services including, but not limited to:

- Enhanced LTE Public Safety grade voice telephony
- Mission Critical Push-To-Talk (MC-PTT)
- Broadcast services for Commercial Mobile Alert System (CMAS)
- Proximity Services (ProSe) and Direct Mode
- MC Data
- MC Machine-to-Machine (M2M)
- MC Location Services – enhanced accuracy for x, y, z direction and indoor locations

A.6.3 Quality of Service, Priority, and Preemption

Provide a detailed description of the strategy and design of the solution for Quality of Service, Priority, and Preemption (QPP) noting how public safety users have guaranteed access to network services in case of emergency and network congestion. Describe the following key QPP service designs for the NPSBN:

- **Quality of Service** – Provide the Quality of Service design and identify Guarantee Bit Rates (GBR) and Maximum Bit Rate (MBR) for GBR bearer, APN-AMBR and UE-AMBR for non-GBR bearer, latency, and packet error loss rate for each service and profile.
- **Priority (Static, Dynamic)** – Provide the design of the static and dynamic priority profiles to support multiple roles with differing priorities and service mixtures.
- **Preemption (Static, Dynamic)** – Provide the design of the static and dynamic pre-emption of an active, low priority user to allow a high priority user to acquire services in the NPSBN during heavy congestion conditions and how to invoke the dynamic priority sequence.

A.7 Network Implementation

Text for this section will be provided by FirstNet.

A.7.1 Integration Partners

Provide an approach for network integration with partners. The integration includes all involved networks (e.g., MVNO, FirstNet Core, Roaming partners, and state-deployed RANs), and a schedule for NPSBN and External Networks, including MVNOs, roaming partners, and state-deployed RANs.

A.7.2 Network Naming and Identification

Provide a description of the design, implementation, and management plan for naming and identification of network nodes for the NPSBN to facilitate a seamless network services implementation and operation. Provide a description of the management approach for identification of public safety devices, RAN equipment, Core network equipment, telephone numbers, tracking areas, proximity-based services, LTE/WLAN interworking, eMBMS service, group multicast calls, and group broadcast calls.

Include a description of the design, implementation and management plan for the naming and identification of at least the following items.

- International Mobile Subscriber Identity (IMSI)
- Public Land Mobile Network Identifier (PLMN)
- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Tracking Area Identifier (TAI)
- Access Point Name (APN)
- Global Unique Temporary UE Identify (GUTI)
- Global Unique MME Identify (GUMMEI)
- Cell Radio Network Temporary Identifier (C-RNTI)
- Packet Data Network Identity (PDN ID)
- EPS Bearer Identifier
- E-RAB Identifier
- Linked EPS Bearer Identifier
- Tunnel End Point Identifier
- International Mobile Equipment Identity (IMEI)
- ADNSF Server Name
- Temporary Mobile Group Identity (TMGI)
- ProSe Application ID
- Fully Qualified Domain Names for Security Gateway and OAM systems

A.7.3 Design Assumptions

Provide assumptions of the design for the NPSBN network implementation. The assumptions shall clearly identify responsible owners. Any impact to quality metrics should be clearly identified in case assumptions are different to implementation. Provide a three- to five-year forecast of assumptions that are relevant to the NPSBN network design.

A.7.4 IP Strategy

Document and provide an IP addressing plan (IPv4 and IPv6). Outline a solution to maintain and manage its IP addresses both public and private as well as the distribution and assignment within the NPSBN, interfacing to external networks and for user devices.

Include an architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC, including but not limited to the following:

- IP design
- Overall IP plan
- IP addressing schema and assignments
- Description of reports that the state will receive, which may include:
    - IP Management plan
    - IP utilization report
- Roadmap according to IOC/ FOC milestones for the IP strategy

A.7.5 Heterogeneous Network Integration

Document and provide a plan to integrate multiple networks (e.g., MVNO, Core, Roaming partners, state deployed RANs) together to form a seamless network implementation and operation. Outline the solution to maintain and manage this heterogeneous network as well as on going network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. Document and provide a roadmap according to IOC/ FOC target milestones for the network integration strategy.

A.7.6 Numbering Plan

Provide a design and implementation plan for the numbering and addressing schema for public safety devices. Provide the ISDN numbering plan, which complies with the United States regulation, to assign public safety devices. Provide a schema on how device numbering will be mapped to user identities (ICAM). In addition, provide a network address approach for packet data communication between public safety devices and mobiles in other networks. The numbering and addressing plan should apply to public safety devices roaming in other PLMNs. Address how the approach supports both IPv4 and IPv6.

Include a description of the architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- Numbering plan
- Numbering design
- Numbering management plan

A.7.7 PSEN and PSAP Integration

Provide the PSEN and PSAP integration plan to the core systems across all integrated networks (e.g. MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network implementation and operation. Provide an ongoing PSEN and PSAP integration plan to grow, maintain, manage, and report on these connections including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments and removals. Provide a roadmap according to IOC/ FOC target milestones for the PSEN and PSAP integration strategy.

Include an architecture, design, maintenance, and management plan for PSEN and PSAP integration for each year during IOC/FOC and after FOC including but not limited to the following:

- Integration and testing schedule
- Integration test plan
- Integration performance report
- Risk and jeopardy mitigation report
- Integration and testing completion report

A.7.8 PSTN, ISP and Peering Integration

Provide the PSTN, ISP and Peering Integration approach to the Core systems across all integrated networks (e.g. MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network

implementation and operation. Provide an ongoing PSTN, ISP and peering integration plan to grow, maintain, manage, and report on these connections including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments and removals. Provide a roadmap according to IOC/ FOC target milestones for the PSTN, ISP, and peering integration strategy.

Include the description of the architecture, design, maintenance, and management plan for PSTN, ISP, and Peering Integration for each year during IOC/FOC and after FOC including but not limited to the following:

- Integration and testing schedule
- Integration test plan
- Description of reports that the state will receive, which may include:
    - Integration performance report
    - Risk and Jeopardy mitigation report
    - Integration and testing completion report

A.7.9 PLMN and Roaming Partner Integration

Provide the PLMN and roaming partner integration approach to the Core systems across all integrated networks (e.g., MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network implementation and operation. Provide an ongoing PLMN and roaming partner integration plan to grow, maintain, manage, and report on these connections including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments and removals. Provide a roadmap according to IOC/ FOC target milestones for the PLMN and roaming partner integration strategy.

Include the description of the architecture, design, maintenance, and management plan for the PLMN and roaming partner integration for each year during IOC/FOC and after FOC including but not limited to the following:

- Integration and testing schedule
- Integration test plan
- Description of reports that the state will receive, which may include:
    - Integration performance report
    - Risk and Jeopardy mitigation report
    - Integration and testing completion report

A.7.10 State-Deployed RAN Integration

Provide a description of the approach to integrating state-deployed RANs and the plan to connect with the Core systems across all integrated networks (e.g., MVNO, Core, Roaming partners, and state-deployed RANs) to form a seamless network implementation and operation. Provide an ongoing state-deployed RAN integration plan to grow, maintain, manage, and report on these connections including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. Provide a roadmap according to IOC/ FOC target milestones for the state-deployed RAN integration strategy.

Include an architecture, design, maintenance, and management plan for the state-deployed RAN integration for each year during IOC/FOC and after FOC including but not limited to the following:

- Integration and testing schedule
- Integration test plan
- Description of reports that the state will receive, which may include:
  - Integration performance report
  - Risk and jeopardy mitigation report
  - Integration and testing completion report

A.7.11 Support for LMR Network Integration

If the Offeror's solution includes future plans for LMR integration, provide a description of the approach and the anticipated timeline.

A.8 Project Plan/Schedule

Provide a detailed project plan and schedule for the implementation of the NPSBN. This includes, but not limited to RAN, Core, Network Services, Transport network, Applications, OSS, BSS systems. Identify any variances with Section J, Attachment J-8, IOC/FOC Target Timeline, and the reasons for those variances. Provide a roadmap according to IOC/ FOC target milestones for the approach for the launch of NPSBN.

Include a description of the architecture, design, maintenance, and management plan for each year during IOC/FOC and after FOC including but not limited to the following:

- NPSBN program plan
- NPSBN implementation plan
- NPSBN integrated project plans and schedules supporting each aspect of the NPSBN program

A.8.1 MVNO to NPSBN Core/RAN Migration

If Offeror's solution includes an MVNO, provide a description of the approach for migrating public safety users from the MVNO model to the NPSBN. This approach may include a number of phases (some of which are identified in Section J, Attachment J-8, IOC/FOC Target Timeline) which includes at least migrating to the Core network, NPSBN applications ecosystem, NPSBN devices, NPSBN services, and finally the schedule rollout of the NPSBN RAN network. The approach will show how mobile number portability will be maintained (see more instruction in the next section) in order to ensure seamless migration.

Include a program and project plan and schedule for each year during IOC/FOC and after FOC including but not limited to the following:

- Migration program plan
- Integrated migration project(s)
- Integrated migration schedule(s)
- Migration completion report

A.8.2 Number Portability

Provide a description of the design for mobile number portability approach. In other words, it is possible to change the IMSI or mobile service provider without changing the ISDN number allocated to a public safety device. Provide the design for the time frame of the porting process in accordance with appropriate FCC TAB RMTR recommendations (Section J, Attachment J-3).

Include a program, project plan and schedule for each year during IOC/FOC and after FOC including but not limited to the following:

- Number portability design
- Number portability program plan
- Number portability project plan
- Number portability schedule
- Number portability completion report

APPENDIX B Device Strategy, Roadmap, and Support

Text for this section will be provided by FirstNet.

B.1 Device Portfolio Available to PSE

Provide a list of the devices that compose the FirstNet device portfolio that are available to a PSE for purchase via the customer facing portal web-based portal.

B.2 Device Acceptance Process

Provide a list of all of the PTCRB certificates that have been supplied by mobile device vendors that have deployed devices on FirstNet.

B.3 Users

Text for this section will be provided by FirstNet.

B.4 Bring Your Own Device Policy

BYOD policy will be defined and provided by FirstNet.

B.5 Device Pricing

Provide the cost of each device in the customer-facing Web-based portal webpage.

B.6 Device Support and Life-Cycle Management

Provide a description of device support, which includes but is not limited to, end user training, end user documentation, and contact information (email addresses, phone numbers, etc.) all via the customer-facing, Web-based portal. Describe the device life-cycle management process.

B.7 Local Control and Management of User Devices

Provide a description of reports that will be made available to the state in support of local control and user device management. These reports may include the following:

- A rolled up summary report of all apps downloaded, a count of all completed OTA updates, a list of the issues with devices and software updates, a list of the issues with shared device updates, and a report on BYOD software updates.
- A report that gives the number of active and inactive UICC in inventory, the number of assigned/unassigned devices in inventory, and the number of UICC and/or devices that are on order or in the return cycle.
- A report that summarizes the updates to applications and content management policies on active devices, indicating how many have successfully updated to each policy and how many failed the update(s).
- The number of OTA updates that have been used for OS/Firmware upgrades sorted by device model and OEM, as well as the number remaining to be upgraded
- A summary of devices that have undergone diagnostics, the number and type of test failures, and the model numbers sorted by OEM.

- The number of single user devices that have been upgraded to each valid software version as well as the number of those that have failed upgrade.
- The number of shared devices that have been upgraded to each valid software version as well as the number of those that have failed upgrade.
- A list of active users and date they were provisioned and de-provisioned from the network as well as the model number and type they were assigned sorted by agency.
- A list of active users and date they were provisioned to the network as well as the model number and type they were assigned sorted by agency.

B.8 Device Support of Network Services

Using the customer-facing, Web-based portal, provide information describing the network services each device supports.

B.9 Device Support of Commercial Band Access to Cellular Service

For each device, specify the commercial cellular bands supported by each device on the customer-facing, Web-based portal.

B.10 Roadmap for Device Support of New Features and Services

Provide a roadmap for future device features and services.

B.11 SIM/UICC Distribution Process and Management

Describe SIM/UICC distribution and management processes.

APPENDIX C Application Strategy and Operations

Text for this section will be provided by FirstNet.

C.1 Baseline Launch Applications

Describe and/or provide examples of how contractor can support (existing business relationships, partnerships, conferences, etc.) the development of value added public safety applications in the following categories:

- By target domain
  - General Purpose (cross domain)
  - Targeted to Law Enforcement
  - Fire
  - Emergency Medical Services domain
- By Connectivity
  - Mobile Device Resident Applications
  - Mobile apps requiring server support
  - Cloud Services and Applications
- By Functionality
  - Network Status/Problem Reporting Applications
  - Virtual Assistant Applications
  - Situational Awareness Applications
  - Computer Aided Dispatch Applications
  - Reference Applications
  - Local Control Applications
  - Command and Control Applications
  - Data Analytics/Crime Analytics
- By Commercial Model
  - Open/Public Applications – Free
  - Open/Public Applications – Free with in-app purchases
  - Commercial Applications – Fee based
  - Commercial Applications - Usage Fee based
- By Security
  - Dimensions of FIPS 199
  - Dimensions of FIPS 200
  - Security as a Service
  - Identity as a Service
  - Mobile Security
  - Mobile VPN
- By Distribution Model
  - Embedded in Device Firmware
  - Pre-installed Locked and Unlocked
  - Downloadable from App Store
  - Distributed through PSEs for Side-loading onto Devices
  - Distributed by PSE MAM/MDM Solution

    - Distributed by FirstNet MAM/MDM Solution
- By Developer Type
    - Certified FirstNet Developer
    - Un-certified Developer
- By Release Date Range
    - With IOC-1
    - Between IOC -1 and IOC-2
- Application Development
    - Best Practices/White Papers/Reference Material
    - Sample/Reference Code
    - Test Cases/Test Plans
    - FirstNet SDK/API for server side support
    - FirstNet SDK/API for mobile platforms
    - Online Training

C.2 Applications Storefront

Provide a plan for the development of the public safety applications marketplace: including the public safety applications available, tracking the number downloads, application ratings for law enforcement, fire and emergency medical services users, measures of application life-cycle management, and operational metrics.

C.3 Applications Management

Provide a plan on building the federated FirstNet ICAM trust framework including ICAM with federated identity from PSE networks, identity assurance, authorization, and credentialing.

C.4 Applications Security

Provide a plan for the security of user data and applications to at least include operational metrics on malware, intrusions, breaches, incidents, and sources of threats.

C.5 Local Control

Provide a plan for deploying local control capabilities including the total trained and certified users and administrators, performance metrics related to latency during provisioning and updating static and dynamic profiles during incidents, and operational metrics. Plan will provide for a real time local view of network status, performance, services and any related trouble ticketing.

C.6 Applications Certification

Provide a plan on the building a vibrant application developer community and application certification pipeline to at least include the total numbers of certified developers, certified applications, failed certifications, certification timelines, and operational metrics.

C.7 Public Safety Entity Home Page

Provide a plan for delivering a Public Safety Entity home page that is customized and managed by the local public safety agencies, and addresses the following:

- Customizable services and data feeds that can be subscribed to including NPSBN status, agency information, alerts, and basic situational awareness of recent nationwide and local incidents.

- Expansion of new features that can be plugged into the Agency Home Page.
- Support for ABAC (Attribute Based Access Control) and the ability for Local Administrators to control the content of what is displayed and to whom.
- Deployment schedule and support plan, and operational metrics for adopting agencies.
- Various mechanisms to alert agencies, such as email, SMS, RSS, FirstNet status page, and any other such "push" alerts.

C.8 Applications Developer and Publication

Provide a plan for building an application development platform to include a catalog of the app development tools, APIs, SDK libraries, application frameworks, testing tools, number of registered application developers, and operational metrics. The plan should also address the following:

C.9 API Taxonomy

Provide a plan for the network, cloud and data services, and the APIs that are available for applications developers to foster new creative public safety applications.

C.10 Applications Product Roadmap

Provide a technology and services evolution roadmap to at least include federated ICAM, local control, network services, application store, cloud services, agency portal, and the application development environment that leverages emerging standards and the commercial marketplace.

APPENDIX D Deployable Assets

Text for this section will be provided by FirstNet.

D.1 Deployable Operations

Describe the operational aspects associated with each deployable type. This should include activation methods, typical time for deployment from request, operations and maintenance required, and associated costs.

D.2 Fleet Management

Describe the fleet management plan for all deployable assets. Including information related to permanent and temporary staging locations (in the event they may be mobilized and pre-staged for hurricane or wildfire seasons, for example) and proposed available quantities of each type of deployable solution.

D.3 Activation

Describe the process for activating deployable assets as required to address coverage and capacity issues.

D.4 Incident Management

Provide a description of how deployable assets will be utilized to address planned events and the five National Incident Management System (NIMS) types for unplanned events, specifically with respect to response time, coverage area and required capacity.

Describe how state-deployed RAN states' deployable units should interact with the NPSBN for scenarios such as a multi-state emergency where assets from state-deployed RAN states may be used to support events in FirstNet-deployed RAN states, and vice-versa.

Note any assumptions regarding State support expected and/or pre-staging of deployable assets. Discuss the involvement of State personnel in the deployment and operation of the equipment.

D.5 Deployable Integration/Backhaul

Describe how deployable units will be integrated into the macro network and with other deployable units from a RAN perceptive to avoid interference and provide handoff communications. In addition, describe integration into the Core network with the types of available backhaul.

D.6 Roles and Responsibilities (State or Territory/FirstNet)

Describe the envisioned roles and responsibilities from public safety entities, FirstNet and Contractor. Include a position on allowing public safety entities to have ownership of deployable assets.

APPENDIX E Financials

E.1 Covered Leasing Agreement/Excess Network Capacity Value

Text for this section will be provided by FirstNet.

E.2 FirstNet Value Proposition

Text for this section will be provided by FirstNet.

E.3 User Fees/Costs

Provide an update of expected user fees and service plan pricing via a resubmission of an updated and current Section J, Attachment 23, End-User Pricing Tables.

E.4 Procurement Vehicles

Text for this section will be provided by FirstNet.

E.5 Funding Allocation for Buildout within the State or Territory

Text for this section will be provided by FirstNet.

E.6 Core Network User Fee

Text for this section will be provided by FirstNet.

E.7 Infrastructure Leasing Fee

Text for this section will be provided by FirstNet.

Table of Contents

1 Terms and Conditions for the Use of FirstNet Network Capacity

1.1 Background

A. The Middle Class Tax Relief and Job Creation Act of 2012 (Pub. L. No. 112-96, Title VI, 126 Stat. 256 (codified at 47 U.S.C. § 1401 *et seq.*)) (the "Act") authorizes the First Responder Network Authority ("FirstNet") to ensure the establishment of a nationwide, interoperable public safety broadband network ("NPSBN").

B. FirstNet is the licensee of station license WQQE234 in the 700 MHz Public Safety Broadband Nationwide License Radio Service issued by the Federal Communications Commission ("FCC" or "Commission") pursuant to the Act, the Communications Act of 1934 (as amended, the "Communications Act"), and the FCC's Rules.

C. The Act permits FirstNet to enter into a public-private arrangement to construct, manage, and operate the NPSBN, the consideration for which includes, in part, permitting access to Network Capacity (defined below), which arrangement is referred to under Section 6208 of the Act as a covered leasing agreement.

D. These Terms and Conditions for the Use of FirstNet Capacity ("Capacity Terms & Conditions") are incorporated into and supplement the terms of the contract and set forth certain terms and conditions regarding the use of the Network Capacity by the Contractor.

1.2 Terms and Conditions

The Contractor shall comply with the following:

1. Defined Terms. For the purposes of these Capacity Terms & Conditions, capitalized terms not otherwise defined herein shall have the following meanings:

   1.1. "Contract" means the written agreement resulting from a public-private arrangement between FirstNet and the Contractor to construct, manage, and operate the NPSBN, including these Capacity Terms & Conditions, which relate to Contractor access to the Network Capacity.

   1.2. "Network Capacity" means the entire capacity of the core network and the Radio Access Network ("RAN") that has been constructed either by FirstNet alone or by the Contractor and is operated, maintained, managed and improved by the Contractor under the Contract, but does not include NPSBN RAN capacity from a state or territory that chooses to conduct its own deployment of a RAN in its state or territory pursuant to Section 1442(e)(2) of the Act.

   1.3. "Public Safety Entity" or "PSE" shall have the meaning ascribed to it in Section 1401(26) of the Act.

1.4. "Regulatory Requirement" means any law, rule, regulation, or ordinance, including but not limited to any applicable rule, regulation, order or decision issued by FirstNet, the FCC, a state Public Utility or Service Commission, a court of competent jurisdiction or other governmental entity.

1.5. "Trademark License" means the separate terms and conditions regarding the use of FirstNet's trade names, trademarks, and service marks.

2. Use of Network Capacity.

2.1. *Public Safety Entity*. The Contractor shall utilize the Network Capacity on a primary basis to provide services to any PSE users. The branding and marketing of services to all PSE users shall be under FirstNet trade names, trademarks, and service marks pursuant to the Trademark License.

2.2. *Non-Public Safety Services*. Subject to Section 2.1 (Public Safety Entity), the Contractor may utilize the Network Capacity on a secondary basis for the provision of non-public safety services in accordance with Section 1428(a)(2)(B) of the Act.

2.3. *Not a Spectrum Lease*. The capacity use right granted under this Section 2 (Use of Network Capacity.) is not a spectrum lease and the Contractor is expressly prohibited from subleasing spectrum authorized to FirstNet under station license WQQE234. Notwithstanding the foregoing, nothing in these Capacity Terms & Conditions is intended to limit the Contractor's ability to team or subcontract with third parties with respect to the build, operation, maintenance, management, and improvement of the NPSBN.

3. Operation of the NPSBN.

3.1. Except for those portions of the NPSBN RAN that a state or territory chooses to construct and operate under Section 1442(e)(2) of the Act, in addition to the rights and obligations under the Contract, the Contractor is directed by FirstNet to manage the NPSBN in accordance with the following:

(i) the Contractor agrees and acknowledges that FirstNet is the licensee of station license WQQE234 and that nothing under these Capacity Terms & Conditions or the Contract shall abrogate FirstNet's control of: (A) the station license WQQE234; or (B) the ultimate responsibility of the operation of the NPSBN which is governed by the terms of the Contract;

(ii) the Contractor shall be responsible for such duties as FirstNet deems necessary in order to facilitate the operation of the NPSBN as further defined in the Contract and which will be reflected in the daily operation of the NPSBN;

(iii) the Contractor agrees and acknowledges that FirstNet shall have unfettered use of and access to all NPSBN facilities and equipment; and

(iv) the Contractor agrees and acknowledges that FirstNet shall make all policy decisions regarding the NPSBN and, subject to Section 4.1, FirstNet will be responsible for filing all FCC applications directly related to FirstNet and station license WQQE234.

3.2. It is expressly agreed and understood that nothing in these Capacity Terms & Conditions is intended to or will constitute a transfer of "control" of station license WQQE234 from FirstNet to Contractor or any other person.

4. Compliance with Regulatory Requirements.

4.1. The Contractor shall be solely responsible for, and accordingly be solely liable for, obtaining and maintaining in its own name and at its own expense, all licenses (except for station license WQQE234), permits, consents, authorizations or other rights required for the use of the Network Capacity, including with respect to the NPSBN and the provision of wireless services to any PSE user or secondary user, and for ensuring compliance with any and all Regulatory Requirements for itself and the operation of the Contractor-managed NPSBN. Contractor shall indemnify and hold FirstNet harmless against any failure to comply with this provision.

4.2. If any Regulatory Requirement has the effect of canceling, changing, or superseding any material term or provision of these Capacity Terms & Conditions, then these Capacity Terms & Conditions will be deemed modified in such a way as FirstNet and the Contractor mutually agree is consistent with the form, intent and purpose of these Capacity Terms & Conditions and is necessary to comply with the Regulatory Requirement.

5. Use of Funds Provided By FirstNet. No funds made available by FirstNet may be used to make payments under a contract to a person or entity who has been, for reasons of national security, barred by any agency of the Federal Government from bidding on a contract, participating in an auction, or receiving a grant or otherwise in violation of Section 1404 of the Act.

6. Transition of PSE Customers. Within twelve months of the execution of the Contract, the Contractor shall prepare for FirstNet's approval a plan for the transition of all of the PSE users, without termination related costs or charges of any kind to such user, to FirstNet or FirstNet's designee upon any termination of the Contract. The plan shall include transition services, which at a minimum will provide a process by which the Contractor will fully transfer the PSE to FirstNet or FirstNet's designee and the ability, at FirstNet's request, for the PSE to continue to receive services from the Contractor after termination but during a transition period. The plan, which shall be reviewed and updated from time to time by the Contractor for FirstNet's approval, shall be an attachment to these Capacity Terms & Conditions and shall be part of, and subject to, the Contract.

7. No Solicitation. Contractor shall not solicit or attempt to solicit, either directly or indirectly, PSE users that purchased or subscribed to public safety related services over the NPSBN for twenty-four months after the termination of the Contract.

8. Assignment. Contractor shall not assign or otherwise transfer these Capacity Terms & Conditions or any rights or obligations hereunder, by operation of law or otherwise, without the prior written consent of FirstNet, and any attempt to do so will be null and void.

9. No Joint Venture. These Capacity Terms & Conditions are not intended to create nor shall it be construed to create any partnership, joint venture, employment or agency relationship between FirstNet and Contractor, and no party shall be liable for the payment or performance of any debts, obligations, or liabilities of the other party, unless expressly assumed in writing herein or otherwise. FirstNet and Contractor each retain full control over the employment, direction, compensation and discharge of their employees, and will be solely responsible for all compensation of such employees, including social security, withholding and worker's compensation responsibilities.

10. No Third-Party Beneficiaries. These Capacity Terms & Conditions are entered into solely among, and may be enforced only by, FirstNet and the Contractor and shall not be deemed to create any rights in any third parties, including suppliers and customers of FirstNet or the Contractor, or to create any obligations of FirstNet or the Contractor to any such third parties.

11. Severability; No Waiver. If any term, covenant or condition in these Capacity Terms & Conditions are, to any extent, invalid or unenforceable in any respect under the Regulatory Requirements governing these Capacity Terms & Conditions, the remainder of these Capacity Terms & Conditions shall not be affected by such invalidity or unenforceability, and each term, covenant or condition of these Capacity Terms & Conditions shall remain valid and enforceable to the fullest extent permitted by law. The failure of either FirstNet or the Contractor to enforce any of the provisions of these Capacity Terms & Conditions, or the waiver of any of the provisions of these Capacity Terms & Conditions in any instance, shall not be construed as a general waiver or relinquishment on its part of that provision. No waiver or modification of any provision of these Capacity Terms & Conditions shall be implied. In order to be effective, a waiver or modification of a provision of these Capacity Terms & Conditions shall be in writing and must be signed by the party against which it is to be enforced.

12. Survival. The expiration or termination of the Contract will not affect the rights or obligations: (i) with respect to Section 6 (Transition of Public Safety Entity Customers) and Section 7 (No Solicitation) of these Capacity Terms & Conditions; or (ii) pursuant to any other provisions of these Capacity Terms & Conditions that, by their sense and context, are intended to survive the expiration or termination of these Capacity Terms & Conditions.

13. Incorporation by Reference; Priority. These Capacity Terms & Conditions are part of and are hereby incorporated into the Contract, which such Contract is permitted and was entered into under the Act and defines the Contractor's rights and obligations regarding the public-private arrangement to build, operate, maintain, manage, and improve the NPSBN. The Contract contains additional terms and conditions to which the Contractor is subject, including with respect to the use of the Network Capacity. Unless expressly provided otherwise in the Contract, in the event of conflict between the Contract and these Capacity Terms & Conditions, the order of priority shall be: (i) these Capacity Terms & Conditions but only with respect to matters specifically addressed herein; and (ii) the Contract.

Attachment to the
Terms and Conditions for the Use of FirstNet Network Capacity

Transition Plan

[To Be Prepared By the Contractor and Approved by FirstNet]

Terms and Conditions for the Trademark Use

Background

A. The Middle Class Tax Relief and Job Creation Act of 2012 (the Act) creates the First Responder Network Authority (FirstNet) to ensure the establishment of the Nationwide Public Safety Broadband Network (NPSBN).

B. The Act permits FirstNet to enter into a public-private arrangement to construct, manage, and operate the NPSBN.

C. Pursuant to the Capacity Terms and Conditions, the services provided to Public Safety Entity users by the Contractor shall be branded and marketed under FirstNet's trade names, trademarks, and service marks (collectively, along with any similar marks or names, or any derivatives of such trade names, trademarks, and service marks, referred to herein as the "Marks").

D. These Terms and Conditions for the Trademark Use ("Trademark Terms & Conditions") set forth certain terms and conditions regarding the use of the Marks by the Contractor and may be supplemented in the contract.

Terms and Conditions

The Contractor shall comply with the following:

1. Defined Terms. For the purposes of these Trademark Terms & Conditions, capitalized terms not otherwise defined herein shall have the following meanings:

    1.1. "Public Safety Entity" or "PSE" shall have the meaning ascribed to it in Section 1401(26) of the Act.

    1.2. "Regulatory Requirement" means any law, rule, regulation, or ordinance, including but not limited to any applicable rule, regulation, order or decision issued by FirstNet, the Federal Communications Commission (FCC), a state Public Utility or Service Commission, a court of competent jurisdiction or other governmental entity.

2. License Grant.

    2.1. Subject to these Trademark Terms & Conditions, for the term of the contract, FirstNet hereby grants to Contractor, and Contractor hereby accepts from FirstNet, a limited, personal, non-exclusive, non-transferable, non-sublicenseable right and license to use the Marks solely and exclusively in connection with the marketing of NPSBN services to Public Safety Entity users within the United States and its designated Territories. Contractor shall use the Marks only to the extent permitted under this license, and except as provided above, neither the Contractor nor any affiliate, owner, director,

officer, employee, or agent thereof shall otherwise use the Marks without the prior express written consent of FirstNet in its sole and absolute discretion. All rights not expressly granted to Contractor hereunder shall remain the exclusive property of FirstNet.

2.2. Nothing in these Trademark Terms & Conditions shall preclude FirstNet from using or permitting other entities to use the Marks.

3. Ownership. Contractor acknowledges that Contractor shall not acquire any right, title, or interest in the Marks by virtue of these Trademark Terms & Conditions other than the license granted hereunder, and disclaims any such right, title, interest, or ownership. Contractor further acknowledges and agrees that FirstNet is the owner of all right, title, and interest in and to the Marks, and all such right, title and interest shall remain with FirstNet. Contractor shall not contest, dispute, challenge, oppose or seek to cancel FirstNet's right, title, and interest in and to the Marks. Contractor shall not prosecute any application for registration of the Marks or seek to register the Marks as a domain name or part of any domain name.

4. Goodwill. All goodwill and reputation generated by Contractor's use of the Marks shall inure to the exclusive benefit of FirstNet. Contractor recognizes the importance of the FirstNet Marks and the Goodwill associated with such Marks and shall take all actions necessary to maintain and further the Goodwill associated with the Marks in the conduct of the services contemplated under the contract. Contractor shall not by any act or omission use the Marks in any manner that disparages or reflects adversely on FirstNet or its business or reputation. Contractor shall not take any action that would interfere with or prejudice FirstNet's ownership or registration of the Marks, the validity of the Marks, or the validity of the license granted by these Trademark Terms & Conditions.

5. Quality Control. In order to preserve the inherent value of the Marks, Contractor agrees to ensure that it maintains the quality of the Contractor's business and the operation thereof equal to the highest standards prevailing in the mobile wireless communications industry in United States during the term of the contract. FirstNet shall oversee the quality of the services provided under the Marks by virtue of its role as the licensee of station license WQQE234, and shall approve, prior to their use, all prospectuses, advertisements, and other materials upon which Contractor uses the Mark. The Contractor further agrees to use the Mark in accordance with such quality and use standards as may be established by FirstNet and communicated to the Contractor, or as may be agreed to by FirstNet and the Contractor, from time to time in writing. In all instances, Contractor shall appropriately include the Marks in accordance with the quality and use guidelines when marketing, offering, selling, or otherwise providing services contemplated under the contract.

6. Notification of Infringement. Contractor shall immediately notify FirstNet and provide to FirstNet all relevant background facts upon becoming aware of: (i) any registrations of, or applications for registration of, marks that do or may conflict with any the Marks; and (ii) any infringements, imitations, or illegal use or misuse of the Marks. FirstNet shall have the exclusive right, but not the obligation, to prosecute, defend and/or settle in its sole discretion, all actions, proceedings and claims involving any infringement or claim, and to take any other action that it deems necessary or proper for the protection and preservation of its rights in the Marks.

Contractor shall cooperate with FirstNet in the prosecution, defense, or settlement of such actions, proceedings, or claims fully and in a timely manner.

7. Effect of Termination. Upon expiration or termination of these Trademark Terms & Conditions or the contract, whichever is earlier, all rights and licenses granted to Contractor under these Trademark Terms & Conditions with respect to the Marks shall cease, and Contractor shall immediately discontinue all use of the Marks.

8. Assignment. Contractor shall not assign or otherwise transfer these Trademark Terms & Conditions or any rights or obligations hereunder, by operation of law or otherwise, without the prior written consent of FirstNet, and any attempt to do so will be null and void.

9. No Joint Venture. These Trademark Terms & Conditions are not intended to create nor shall it be construed to create any partnership, joint venture, employment or agency relationship between FirstNet and Contractor, and no party shall be liable for the payment or performance of any debts, obligations, or liabilities of the other party, unless expressly assumed in writing herein or otherwise. FirstNet and Contractor each retain full control over the employment, direction, compensation and discharge of their employees, and will be solely responsible for all compensation of such employees, including social security, withholding and worker's compensation responsibilities.

10. No Third Party Beneficiaries. These Trademark Terms & Conditions are entered into solely among, and may be enforced only by, FirstNet and the Contractor and shall not be deemed to create any rights in any third parties, including suppliers and customers of FirstNet or the Contractor, or to create any obligations of FirstNet or the Contractor to any such third parties.

11. Severability; No Waiver. If any term, covenant or condition in these Trademark Terms & Conditions are, to any extent, invalid or unenforceable in any respect under the Regulatory Requirements governing these Trademark Terms & Conditions, the remainder of these Trademark Terms & Conditions shall not be affected by such invalidity or unenforceability, and each term, covenant or condition of these Trademark Terms & Conditions shall remain valid and enforceable to the fullest extent permitted by law. The failure of either FirstNet or the Contractor to enforce any of the provisions of these Trademark Terms & Conditions, or the waiver of any of the provisions of these Trademark Terms & Conditions in any instance, shall not be construed as a general waiver or relinquishment on its part of that provision. No waiver or modification of any provision of these Trademark Terms & Conditions shall be implied. In order to be effective, a waiver or modification of a provision of these Trademark Terms & Conditions shall be in writing and must be signed by the party against which it is to be enforced.

12. Incorporation by Reference; Priority. These Trademark Terms & Conditions are part of and are hereby incorporated into the contract, which such contract is permitted and was entered into under the Act and defines the Contractor's rights and obligations regarding the public-private arrangement to build, operate, maintain, manage, and improve the NPSBN. The contract contains additional terms and conditions to which the Contractor is subject, including with respect to the use of the Marks. Unless expressly provided otherwise in the contract, in the event of conflict between the contract and these Trademark Terms & Conditions, the order of

priority shall be: (i) these Trademark Terms & Conditions but only with respect to matters specifically addressed herein; and (ii) the contract.

13. Termination or Suspension. To the extent permitted by applicable law, FirstNet may terminate, or in its discretion, suspend this License immediately by written notice to Contractor upon (a) the institution by Contractor of insolvency or bankruptcy proceedings or any other act of bankruptcy or proceedings for the settlement of its debts; (b) the institution of such proceedings against Contractor, which is not dismissed or otherwise resolved in its favor within sixty (60) days thereafter; (c) Contractor making a general assignment for the benefit of creditors; (d) any attempted assignment of this license by Contractor, (e) any failure of Contractor to strictly adhere the terms of this license, including any quality or use standards required by FirstNet hereunder, which failure is not cured to FirstNet's satisfaction within fifteen (15) days of the date on which such failure is discovered; or (f) any breach of the contract terms not cured within the applicable periods afforded by the contract terms.

14. Audit Rights. FirstNet shall have the right upon reasonable prior notice to audit Contractor's use of the Marks in accordance with this license and shall be granted full access to all related information, personnel and documentation in order for FirstNet to verify compliance with the License terms. All inspection shall take place at the Contractor's headquarters, or other location as mutually agreed by the parties, and shall be conducted during normal business hours. If no location is made available by the Contractor then all necessary information shall be made available for inspection at a time and location convenient to FirstNet. The cost of the audit shall be borne by FirstNet unless it is determined that Contractor is in violation of any License terms in which case Contractor shall be responsible to reimburse FirstNet for all incurred expenses within sixty (60) days of communication by FirstNet of the audit findings.

Offeror Name _____

Solicitation Reference		Proposal Reference			
Section #	**Requirement**	**Contractor Self Certification**	**Page #**	**Section #**	**Brief Description**
L.1.7	Disclosure statement regarding the use of current or previous Government employees in the proposal process and/or resultant contract *(if applicable)*	☐ Meets ☐ Does Not Meet			
L.2.4	Submission of Capability Statements *(One original hard copy, eight hard copies, and soft copies on three flash drives, per instructions and specified due date/time)*	☐ Meets ☐ Does Not Meet			
L.2.5	Submission of Proposals *(One original hard copy, eighteen hard copies, and soft copies on two flash drives, per instructions and specified due date/time)*	☐ Meets ☐ Does Not Meet			
L.3	Submission of Proposal in Three Volumes • Volume 1: Business Management • Volume 2: Technical • Volume 3: Pricing *(Submitted per formatting and page length and additional instructions)*	☐ Meets ☐ Does Not Meet			
L.3.1.5.1	Financial Resources • Financial Statements • Credit Ratings • Material Changes in Financial Conditions	☐ Meets ☐ Does Not Meet			

Solicitation Reference		Proposal Reference			
Section #	**Requirement**	**Contractor Self Certification**	**Page #**	**Section #**	**Brief Description**
L.3.2.1.1.6	Planning Tool Analysis Layers: Esri shapefiles and MapInfo files *(Submitted per delivery method instructions)*	☐ Meets ☐ Does Not Meet			
L.3.2.1.1, L.3.2.1.3.1	Initial Operational Capability (IOC)/Final Operational Capability (FOC) Coverage Maps: Esri shapefiles and MapInfo files *(Submitted per delivery method instructions)*	☐ Meets ☐ Does Not Meet			
J-2	Nationwide and Rural Coverage Compliance Checklist	☐ Meets ☐ Does Not Meet			
J-9	Quality Assurance Surveillance Plan (QASP) Surveillance Matrix Template	☐ Meets ☐ Does Not Meet			
J-11	Device Specifications Template	☐ Meets ☐ Does Not Meet			
J-12	Test Strategy Template	☐ Meets ☐ Does Not Meet			
J-13	Pricing Template	☐ Meets ☐ Does Not Meet			
J-15	Contractor-Furnished Equipment Table	☐ Meets ☐ Does Not Meet			
J-16	Deliverables Table	☐ Meets ☐ Does Not Meet			
J-17	Coverage and Capacity Template	☐ Meets ☐ Does Not Meet			
J-22	Solicitation Conformance Traceability Matrix *(This document)*	☐ Meets ☐ Does Not Meet			

Solicitation Reference		Proposal Reference			
Section #	Requirement	Contractor Self Certification	Page #	Section #	Brief Description
J-23	End-User Pricing Tables	☐ Meets ☐ Does Not Meet			
J-24	Public Safety Device Connections Template	☐ Meets ☐ Does Not Meet			
J-25	Past Performance Reference Information Form	☐ Meets ☐ Does Not Meet			

Table of Contents

List of Tables

1 End-User Pricing Tables

Table 1 End-User Service Pricing – Post-Paid and Table 2 End-User Service Pricing – Pre-Paid represent indicative pricing to public safety users. When completing the tables, the Offeror shall take into account any assumptions used in determining indicative pricing, such as details on usage caps, roaming caps, throttling, and contract length. Additionally, the Offeror shall indicate the proposed volume discount schedule and special pricing mechanisms to support public safety adoption and use of the Nationwide Public Safety Broadband Network. The Offeror shall use Table 3 Public Safety Devices and Estimated Price Points to identify the anticipated supplier and estimated price points for Band 14-enabled devices for public safety.

Table 1 End-User Service Pricing – Post-Paid

Plan Description (Post-Paid)	Measure	Pricing
Metered Monthly Recurring Charge (MRC)	MRC	
Metered Usage per Gigabyte (GB)	GB	
5 GB Pooled	MRC	
50 GB Pooled	MRC	
100 GB Pooled	MRC	
500 GB Pooled	MRC	
1000 GB Pooled	MRC	
Pooled Overage	GB	
Unlimited	MRC	
Public Safety Features		
Priority Services	Determined by Offeror	
Preemption	Determined by Offeror	
Additional Public Safety Features	Determined by Offeror	
Tethering	MRC	
Voice	Determined by Offeror	
Text	Determined by Offeror	
Other	Determined by Offeror	

Table 2 End-User Service Pricing – Pre-Paid

Plan Description (Pre-Paid)	Measure	Pricing
Metered Monthly Recurring Charge (MRC)	MRC	
Metered Usage per GB	GB	
5 GB Pooled	MRC	
50 GB Pooled	MRC	
100 GB Pooled	MRC	
500 GB Pooled	MRC	
1000 GB Pooled	MRC	
Pooled Overage	GB	
Unlimited	MRC	
Public Safety Features		
Priority Services	Determined by Offeror	
Preemption	Determined by Offeror	
Additional Public Safety Features	Determined by Offeror	
Tethering	MRC	
Voice	Determined by Offeror	
Text	Determined by Offeror	
Other	Determined by Offeror	

Table 3 Public Safety Devices and Estimated Price Points

Type of Device	Supplier	Anticipated Price to Public Safety
Smartphones		
Ruggedized Devices		
Vehicle Network System		
Femtocell		
Tablets		
Mobile Hot Spots		
USB Modems		
Embedded Modules		
Other Devices		

Past Performance Reference Information Form

1. Complete name of Government agency, commercial firm, or other organization	
2. Complete address	
3. Contract number or other reference	4. Date of contract
5. Date work was begun	6. Date work was completed
7. Estimated contract price	8. Final amount invoiced or amount invoiced to date
9a. Technical point of contact (name, title, address, telephone number, and email address)	9b. Contracting or purchasing point of contact (name, title, address, telephone number, and email address)
10. Location(s) of work (country, state or province, county, city)	
11. Description of contract work (Describe the nature and scope of the experience and provide an explanation of how the work is the same as or similar to the work required by this Request for Proposal). Attach an explanation of any performance problems or other conflicts with the customer. Use a continuation sheet, if necessary.	

Past Performance Reference Information Form

12. Current status of contract (choose one):

☐Work continuing, on schedule
☐Work continuing, behind schedule
☐Work completed, no further action pending or underway
☐Work completed, claims negotiations pending or underway
☐Work completed, litigation pending or underway
☐Terminated for convenience
☐Terminated for default
☐Other (explain)

Instructions for Completing the Past Performance Reference Information Form

- **Item 1** – Insert the complete name of the Government agency, commercial firm, or other organization for which the work was performed.
- **Item 2** – Insert the customer's complete address, including both post office box and street addresses, if applicable.
- **Item 3** – Insert any contract number or other contract reference used by the customer.
- **Item 4** – Insert the date on which the contract came into existence.
- **Item 5** – Insert the date on which you started to perform the work.
- **Item 6** – Insert the date on which the customer agreed that the work was satisfactorily completed. If work is ongoing, insert the date the contract will expire.
- **Item 7** – Insert the total estimated contract price or value.
- **Item 8** – Insert the final sum of all invoices or the sum of all invoices to date.
- **Item 9a** – Insert the name, title, address, telephone number, and email address (if available) of the program or project manager or other customer technical representative who is most familiar with the quality of your work under the contract.
- **Item 9b** – Insert the name, title, address, telephone number, and email address (if available) of the Contracting Officer, purchasing agent, or other customer contracting or purchasing representative who is most familiar with your work under the contract.
- **Item 10** – Insert the location(s) where the work was performed.
- **Item 11** – Describe the nature and scope of the work. The objective is to show how the work that you did or are doing is similar in nature and scope to the work that is to be performed under the contract contemplated by the Request for Proposals. Describe any unusual circumstances of performance or problems that may be relevant to the work that is to be performed. Describe any conflicts with the customer or reasons they may make adverse remarks about your performance. Describe any actions that you have taken to correct any shortcomings in your performance.
- **Item 12** – Check the appropriate box according to the current status of the work.

Table of Contents

Sample Small Business Subcontracting Plan

1 Subcontracting Plan Outline

The following outline meets the minimum requirements of Public Law 95-507 and the Federal Acquisition Regulation (FAR) Subparts 19.7. It is intended to be a guideline. It is not intended to replace any existing corporate plan which is more extensive. If assistance is needed to locate small business sources, contact the Department of the Interior, Small Business Representative at 202-208-3493. Please note that the Department of Commerce, has subcontracting goals of 37% for small business; 5% for small disadvantaged business, 3% for HubZone certified, 5% for women—owned, and 3% for service disabled veteran owned small business for fiscal year 2015.

1.1 Identification Data

Company Name			
Address			
Date Prepared		**Solicitation number**	
Item/Service			
Place of Performance			

1.2 Type of Plan

Check only one

	Plan Type	Plan Description
☐	Individual Plan	In this type of plan, all elements are developed specifically for this contract and are applicable for the full term of this contract.
☐	Master Plan	In this type of plan, goals are developed for this contract; all other elements are standard. The master plan must be approved annually. Once incorporated into a contract with specific goals, it is valid for the life of the contract.
☐	Commercial Products Plan	This type of plan is used when the contractor sells large quantities of off-the-shelf commodities to many Government agencies. Plans/goals are negotiated with the initial agency on a company—wide basis rather than for individual contracts. The plan is effective only during year approved. The contractor must provide a copy of the initial agency approval, AND MUST SUBMIT A SUMMARY SUBCONTRACT REPORT (SSR) FOR "INDIVIDUAL" SUBCONTRACTING PLANS VIA THE ELECTRONIC SUBCONTRACTING REPORT SYSTEM (eSRS).

1.3 Goals

FAR 19.704(a)(1) requires separate dollar and percentage goals for using small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns as subcontractors for the base year and each option year. Goals for subcontracts with small women-owned business concerns are encouraged.

1. Estimated dollar value of all planned subcontracting i.e., to all types of business concerns under this Contract is:

Base	1st Option	2nd Option	3rd Option
$	$	$	$

2. Estimated dollar value* and percentage of planned subcontracting to small business concerns is: *(*This figure includes the amount in 3, 4, 5, and 6 below.)*

Base	1st Option	2nd Option	3rd Option
$	$	$	$
%	%	%	%

3. Estimated dollar value and percentage of planned subcontracting to small disadvantaged business concerns is:

Base	1st Option	2nd Option	3rd Option
$	$	$	$
%	%	%	%

4. Estimated dollar value and percentage of planned subcontracting to small women-owned business concerns is:

Base	1st Option	2nd Option	3rd Option
$	$	$	$
%	%	%	%

5. Estimated dollar value and percentage of planned subcontracting to HubZone certified business concerns is:

Base	1st Option	2nd Option	3rd Option
$	$	$	$
%	%	%	%

6. Estimated dollar value and percentage of planned subcontracting to service disabled veteran owned small business concerns is:

Base	1st Option	2nd Option	3rd Option
$	$	$	$
%	%	%	%

*****IF ANY CONTRACT HAS MORE THAN THREE OPTIONS, PLEASE ATTACH ADDITIONAL SHEETS SHOWING DOLLAR AMOUNTS AND PERCENTAGES***

7. Products and/or services to be subcontracted under this contract, and the types of businesses supplying them, are: *(Check all that apply).*

SUBCONTRACTED PRODUCT/SERVICE	Business Category or Size					
	Large	Small	Small Disadvantaged	Women Owned	HubZone Certified	Service Disabled veteran owned

(ATTACH ADDITIONAL SHEETS IF NECESSARY.)

8. Explain the methods used to develop the subcontracting goals for small, small disadvantaged, and small women-owned business concerns. Explain how the product and service areas to be subcontracted were established, how the areas to be subcontracted to small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone were determined, and how the capabilities of small, small disadvantaged and small women-owned businesses were determined. Identify all source lists used in the determination process.

9. Indirect and overhead costs
   ☐ have been ☐ have not been
   included in the dollar and percentage subcontracting goals stated above. *(Check one.)*

10. If indirect and overhead costs HAVE BEEN included, explain the method used to determine the proportionate share of such costs to be allocated as subcontracts to small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns.

1.4 Program Administrator

FAR 19.704(a)(7) requires information about the company employee who will administer the subcontracting program. Please provide the name, title, address, phone number, position within the corporate structure and the duties of that employee.

Program Administrator	
Name	
Title/Position	
Address	
Telephone	
Duties	*Does the individual named above perform the following?*
☐Yes ☐No	A. Developing and Promoting company/division policy statements that demonstrate the company's/division's support for awarding contracts and subcontracts to small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns
☐Yes ☐No	B. Developing and maintaining bidders' lists of small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns from all possible sources
☐Yes ☐No	C. Ensuring periodic rotation of potential subcontractors on bidders' lists
☐Yes ☐No	D. Assuring that small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone are included on the bidders' list for every subcontract solicitation for products and services they are capable of providing
☐Yes ☐No	E. Ensuring that subcontract procurement "packages" are designed to permit the maximum possible participation of small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone businesses
☐Yes ☐No	F. Reviewing subcontract solicitations to remove statements clauses, etc., which might tend to restrict or prohibit small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business participation

Program Administrator	
☐Yes ☐No	G. Ensuring that the subcontract bid proposal review board documents its reasons for not selecting any low bids submitted by small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns
☐Yes ☐No	H. Overseeing the establishment and maintenance of contract and subcontract award records
☐Yes ☐No	I. Attending or arranging for the attendance of company counselors at Business Opportunity Workshops, Minority Business Enterprise Seminars, Trade Fairs, etc.
☐Yes ☐No	J. Directly or indirectly counseling a small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns on subcontracting opportunities and how to prepare responsive bids to the company
☐Yes ☐No	K. Providing notice to subcontractors concerning penalties for misrepresentations of business status as small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone for the purpose of obtaining a subcontract that is to be included as part or all of a goal contained in the contractor's subcontracting plan
☐Yes ☐No	L. Conducting or arranging training for purchasing personnel regarding the intent and impact of Public Law 95-907 on purchasing procedures
☐Yes ☐No	M. Developing and maintaining an incentive program for buyers which supports the subcontracting program
☐Yes ☐No	N. Monitoring the company's performance and making any adjustments necessary to achieve the subcontract plan goals
☐Yes ☐No	O. Preparing and submitting timely reports
☐Yes ☐No	P. Coordinating the company's activities during compliance reviews by Federal agencies
☐Yes ☐No	Q. Encouraging subcontracting in Labor Surplus Areas when consistent with the efficient performance of the contract

1.5 Equitable Opportunity

FAR 19.704(a)(8) requires a description of the efforts your company will make to ensure that small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone small business concerns will have an equitable opportunity to compete for subcontracts. *(Check all that apply.)*

1. Outreach efforts to obtain sources:

☐	Contacting minority, woman-owned, and small business trade associations
☐	Contacting business development organizations
☐	Attending small, woman-owned, and minority business procurement conferences and trade fairs
☐	Use the Business Partner Network (BPN). BPN is a procurement related Internet-based electronic search engine for locating SB, SDB, WOSB, HUBZ, SDVS, VOSB sources. BPN is a free electronic search mechanism that provides unprecedented views into several key databases across Federal Agencies. Another helpful Internet-based site is the Small Business Administration's Subcontracting Opportunities Directory.

2. Internal efforts to guide and encourage purchasing personnel:

☐	Presenting workshops, seminars and training programs
☐	SB, SDB, WOSB, HUBZ, SDVO, and VOSB concerns source lists, guides, and other data identifying SB, SDB, WOSB, HUBZ, SDVS, and VOSB concerns will be maintained and utilized by buyers in soliciting subcontracts.
☐	Monitoring activities to evaluate compliance with the subcontracting plan

3. Additional efforts: (Please describe.)

1.6 Clause Inclusion and Flow Down

Far 19.704(a)(9) requires that your company to include FAR 52.219-8, "Utilization of Small Business Concerns," in all subcontracts that offer further subcontracting opportunities. Your company must require all subcontractors, except small business concerns, that receive subcontracts in excess of $650,000 ($1,500,000 for construction) to adopt and comply with a plan similar to the plan required by FAR 52.219-9, "Small Business Subcontracting Plan."

Your company agrees that the clause will be included and that the plans will be reviewed against the minimum requirements for such plans. The acceptability of percentage goals for small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns must be determined on a case-by-case basis depending on the supplies and services involved, the availability of potential small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone subcontractors and prior experience. Once the plans are negotiated, approved, and implemented, the plans must be monitored through the submission of periodic reports, including the Individual Subcontract Report (ISR) and the Summary Subcontract Report (SSR) using the eSRS (http://www.esrs.gov).

1.7 Reporting and Cooperation

FAR 19.704(a)(10) requires that your company (1) cooperate in any studies or surveys as may be required, (2) submit periodic reports which show compliance with the subcontracting plan; (3) submit the ISR, and SSR in accordance with the instructions at the eSRS (accessible at http://www.esrs.gov); and (4) ensure that subcontractors agree to submit the ISR and SSR.

1.8 Recordkeeping

FAR 19.704(a)(11) requires a list of the types of records your company will maintain to demonstrate the procedures adopted to comply with the requirements and goals in the subcontracting plan. *(Check all that apply.)*

☐Yes ☐No	A. Small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concern source lists, guides, and other data identifying such vendors
☐Yes ☐No	B. Organizations contacted for small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business sources
☐Yes ☐No	C. On a contract-by-contract basis, records on all subcontract solicitations over $150,000 which indicate for each solicitation (1) whether small business concerns were solicited, and if not, why not; (2) whether small disadvantaged business concerns were solicited,, and if not, why not; (3) whether women-owned small business concerns were solicited, and if not, why not; (4) whether veteran-owned small business concerns were solicited, and if not, why not; (5) whether service disabled veteran-owned small business concerns were solicited, and if not, why not; (6) whether HUBZone small business concerns were solicited, and if not, why not; (7) reasons for the failure of solicited small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns to receive the subcontract award
☐Yes ☐No	D. Records to support other outreach efforts, e.g., contacts with minority and small business trade associations, attendance at small and minority business procurement conference and trade fairs
☐Yes ☐No	E. Records to support internal activities to (1) guide and encourage purchasing personnel, e.g., workshops, seminars, training programs, incentive awards; and (2) monitor activities to evaluate compliance
☐Yes ☐No	F. On a contract-by-contract basis, records to support subcontract award data including the name, address and business size and ownership status (SDB, WOB, etc.) of each subcontractor (This item is not required for company or division-wide commercial products plans.)
	G. Other records to support your compliance with the subcontracting plan: (Please describe)

1.9 Timely Payment to Subcontractors

FAR 19.702 requires your company to establish and use procedures to ensure the timely payment of amounts due pursuant to the terms of your subcontracts with small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns.

Please indicate if company has established and uses such procedures:
☐ Yes ☐ No

1.10 Description of Good Faith Effort

Maximum practicable utilization of small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business concerns as subcontractors in Government contracts is a matter of national interest with both social and economic benefits. When a contractor fails to make a good faith effort to comply with a subcontracting plan, these objectives are not achieved and 15 U.S.C. 637(d) (4) (F) directs that liquidated damages shall be paid by the contractor. In order to demonstrate your compliance with a good faith effort to achieve the small, small disadvantaged, women-owned, veteran-owned, service disabled veteran-owned, and HUBZone business subcontracting goals, outline the steps your company plans to take. These steps will be negotiated with the contracting officer prior to approval of the plan.

1 Parental Guarantee

[GUARANTEE], dated as of _____ __, 20__ (this "Guarantee"), made by [COMPANY], a company organized under the laws of [JURISDICTION] (the "Guarantor"), in favor of the First Responder Network Authority on behalf of the United States Government (the "Government").

RECITALS:

WHEREAS, [CONTRACTOR], a [ENTITY TYPE] organized and existing under the laws of [JURISDICTION] (the "Subsidiary" or "Contractor"), is a subsidiary of the Guarantor;

WHEREAS, the Subsidiary and the Guarantor are related businesses; and

WHEREAS, for the Government to make an affirmative determination of Contractor responsibility, the Guarantor is entering into this Guarantee to ensure that adequate resources are available to the Subsidiary to successfully perform the Subsidiary's obligations under the Agreement;

NOW THEREFORE, the Guarantor agrees for the benefit of the Government as follows:

1. Defined Terms. Capitalized terms not otherwise defined herein shall have the same meanings ascribed to them in the Agreement. The following terms shall have the following meanings when used in this Guarantee:

   "Agreement": the written contract between the Government and Contractor to construct, manage, and operate the Nationwide Public Safety Broadband Network.

   "Guarantor": as defined in the preamble hereto, together with its successors and assigns (whether by way of merger, sale of capital stock, sale of assets, or otherwise).

   "Person": an individual, partnership, corporation, business trust, joint stock company, trust, unincorporated association, joint venture, governmental authority, or other entity of whatever nature.

   "Taxes": taxes imposed on the Government's net income, or franchise taxes imposed on the Government by the jurisdiction under the laws of which it is organized or any political subdivision thereof, and including any withholding made with respect to Taxes.

2. The Guarantor hereby unconditionally and irrevocably guarantees to the Government the due and punctual performance and observance by Contractor of all its respective obligations, commitments, undertakings, warranties, indemnities, and covenants under or in connection with the Agreement (the "Obligations"), and agrees to indemnify the Government on demand against all losses, damages, costs, and expenses (including reasonable legal costs and expenses in respect of any enforcement of the Obligations and/or this Agreement) that the Government may suffer through or that may arise from any breach or failure to perform by Contractor of the Obligations. The liability of the Guarantor as aforesaid shall not be released or diminished by any alterations or modifications of terms or any forbearance, neglect, or delay in seeking performance of the Obligations thereby imposed or any granting of time for such performance or any other indulgence, provided, however,

that the Guarantor's Obligations under this Agreement shall be subject to any such alteration, extension of time, or other indulgence, or any waiver that may be granted.

3. If and whenever Contractor defaults in the performance of the Obligations and such default is not cured or remedied within the time limits provided after notice by the Government to Contractor (within any cure periods—howsoever described, and if any—in the Agreement) ("Default"), the Guarantor shall upon demand, which shall reasonably and briefly specify the nature and amount, if any, of the Default (the "Demand"), unconditionally perform (or procure performance of) and satisfy (or procure the satisfaction of), in accordance with the terms and conditions of the Agreement, the Obligations in regard to which such Default has been made, and so that the same benefits shall be conferred on the Government as it would have received if such Obligations had been duly performed and satisfied by Contractor. The Guarantor hereby waives any rights that it may have to require the Government to proceed first against or claim payment from Contractor, to the extent that as between the Government and the Guarantor, the latter shall be liable as principal obligor upon any aforesaid Default, as if it had entered into all the Obligations jointly and severally with Contractor.

4. This Guarantee is to be a continuing security to the Government for all the Obligations of Contractor notwithstanding any settlement of account or other matter or thing whatsoever. Except to the extent otherwise specifically contemplated herein, the Guarantor waives diligence, presentment and protest, or other notice of any kind with respect to all Obligations. This Guarantee shall be construed as a continuing guarantee of performance of all Obligations owing to the Government by Contractor under the Agreement and not a guarantee of collection.

5. This Guarantee is in addition to and without prejudice to and not in substitution for any rights or security that the Government may now or hereafter have or hold for the performance and observance of the Obligations of Contractor.

6. In the event that the Guarantor has taken or takes any security from Contractor in connection with this Guarantee, the Guarantor hereby undertakes to hold the same in trust for the Government pending discharge in full of all the Guarantor's Obligations under or in connection with the Agreement. The Guarantor shall not, after any Demand has been made hereunder, claim from Contractor any sums that may be owing to it from Contractor or have the benefit of any set-off or counter-claim or proof against, or dividend, composition, or payment by Contractor until all sums owing to the Government hereunder or under or in connection with the Agreement have been paid in full.

7. As a separate and independent stipulation, the Guarantor agrees that any Obligations that may not be enforceable against or recoverable from Contractor by reason of:

   (a) any legal limitation, disability, or incapacity of Contractor or the Guarantor;

   (b) any insolvency or liquidation of Contractor;

   (c) any merger, amalgamation, or other change of status of the Guarantor; or

   (d) any other fact or circumstance,

shall nevertheless be enforceable against or recoverable from the Guarantor as though the same had been incurred by the Guarantor as principal obligor in respect thereof and shall be performed or paid by the Guarantor on demand in accordance with and subject to the provisions of the Agreement.

8. Notwithstanding any other provisions of this Agreement, the Obligations and liability of the Guarantor under or arising out of this Guarantee shall not be interpreted as imposing greater Obligations and liabilities on the Guarantor than are imposed on Contractor under the Agreement.

9. This Guarantee shall remain in full force and effect and be binding upon the Guarantor and its successors and assigns, and shall inure to the benefit of the Government until all the Obligations owing to the Government and the obligations of the Guarantor under this Guarantee shall have been satisfied by performance in full.

10. The Guarantor warrants and confirms to the Government:

    (a) it is duly organized and validly exists under the laws of its jurisdiction of organization and has the power and authority and legal right to own and operate its property and to conduct the business in which it is currently engaged;

    (b) it has the power, authority, and legal right to execute and deliver, and to perform its Obligations under this Guarantee and has taken all necessary action to authorize its execution, delivery, and performance of this Guarantee, and this Guarantee has been duly executed;

    (c) this Guarantee constitutes a legal, valid, and binding obligation of the Guarantor, enforceable in accordance with its terms, subject to the effects of bankruptcy, solvency, reorganization, moratorium, and other similar laws relating to or affecting creditors' rights generally, general equitable principles (whether considered in a proceeding in equity or at law), and an implied covenant of good faith and fair dealing;

    (d) the execution, delivery, and performance of this Guarantee will not violate or result in default in any applicable law, rule, or regulation or any judgment, order, or decree or agreement, instrument, or undertaking applicable to the Guarantor and will not result in, or require, the imposition or creation of any lien on any of its properties or revenues pursuant to any of the foregoing, in each case in any material respect;

    (e) no consent or authorization of, or filing or registration with, any governmental authority, and no consent of any other Person, is required in connection with the execution, delivery, performance, validity, or enforceability of this Guarantee, other than as may have been obtained or made and is in full force and effect;

    (f) there are no laws in effect in the jurisdiction in which the Guarantor is organized and principally conducts its business that limit its maximum liability, except for laws limiting the ability of the Guarantor to incur liabilities that render it insolvent, unable to pay its debts as they become due, or with insufficient or too small capital and except for laws requiring approvals, consents, authorizations, or registrations that have been obtained or made

(except where failure to obtain or make such approvals, consents, authorizations, or registrations would not have a material adverse effect on the ability of the Guarantor to perform its Obligations hereunder); and

(g) it is not entitled to immunity from judicial proceedings and agrees that, in the event the Government brings any suit, action, or proceeding to enforce any Obligation or liability of the Guarantor arising, directly or indirectly, out of or relating to this Guarantee, no immunity from such suit, action, or proceeding will be claimed by or on behalf of the Guarantor.

11. It is a condition of the execution of the Agreement that the Guarantor execute and deliver this Guarantee. The Guarantor acknowledges and agrees that the execution of the Agreement by the Contractor is in the Guarantor's best interests. The Guarantor makes this Guarantee knowing that the Government shall rely on this Guarantee in entering into the Agreement. The Guarantor conclusively acknowledges that the Government's reliance hereon is in every respect justifiable and the Guarantor received adequate and fair equivalent value for this Guarantee.

12. This Guarantee shall be reinstated if at any time any payment of any Obligations must be returned by the Government upon the insolvency, bankruptcy, dissolution, liquidation, or reorganization of the Subsidiary or the Guarantor.

13. The Guarantor agrees that the Obligations owing to the Government shall be paid to the Government in the currency and at the location specified in the Agreement.

14. All notices and demands to or upon the Government or the Guarantor to be effective shall conform to the notice requirements in the Agreement, provided the Government shall provide any required notice to the Guarantor at:

    [ADDRESS/CONTACT]

15. Amendments in Writing; No Waiver; Cumulative Remedies.

    (a) Except as otherwise provided herein, none of the terms or provisions of this Guarantee may be waived, amended, supplemented, or otherwise modified except by a written instrument executed by the Guarantor and the Government.

    (b) The Government shall not by any act (except by a written instrument pursuant to Section 15(a)) or by any delay, indulgence, or omission be deemed to have waived any right or remedy hereunder. No failure to exercise, nor any delay in exercising on the part of the Government, any right, power, or privilege hereunder shall operate as a waiver thereof. No single or partial exercise of any right, power, or privilege hereunder shall operate as a waiver thereof. No single or partial exercise of any right, power, or privilege under this Guarantee shall preclude any other or further exercise thereof or the exercise of any other right, power, or privilege. A waiver by the Government of any right or remedy on any occasion shall not be construed as a bar to any right or remedy that the Government would otherwise have on any future occasion.

16. Submission To Jurisdiction; Waivers.

(a) The Guarantor irrevocably and unconditionally:

(i) submits for itself and its property in any legal action or proceeding relating to this Guarantee, or for recognition and enforcement of any judgment in respect of this Guarantee, to the non-exclusive general jurisdiction of the United States Court of Federal Claims and in each case the appellate courts thereto;

(ii) consents that any such action or proceeding may be brought in such courts and waives any objection that it may now or hereafter have to the venue of any such action or proceeding in any such court or that such action or proceeding was brought in an inconvenient court, and agrees not to plead or claim the same;

(iii) agrees that service of process in any such action or proceeding may be effected by mailing a copy thereof by registered or certified mail (or any substantially similar form of mail), postage prepaid, to the Guarantor as provided in Section 14; and

(iv) agrees that nothing in this Section shall affect the right of the Government to effect service of process in any other manner permitted by law or shall limit its right to sue in any other jurisdiction.

(b) The consent to personal jurisdiction set forth herein shall be self operative and no further instrument or action, other than service of process as provided for herein, shall be necessary in order to confer jurisdiction upon the Guarantor in any such court.

(c) Provided that service of process is effected upon the Guarantor in the manner prescribed by law, the Guarantor irrevocably waives, to the fullest extent permitted by law, and agrees not to assert, by way of motion, as a defense or otherwise:

(i) any objection that it may have or may hereafter have to the laying of the venue of any such suit, action, or proceeding brought in such a court as is mentioned in the previous paragraph;

(ii) any claim that any such suit, action, or proceeding brought in such a court has been brought in an inconvenient forum; or

(iii) any claim that is not personally subject to the jurisdiction of the above-named courts.

17. Taxes. Any and all payments by the Guarantor hereunder shall be made free and clear of and without deduction for any and all present or future fees, levies, imposts, deductions, charges or withholdings, and all liabilities with respect thereto, excluding any Taxes. If the Guarantor shall be required by law to deduct any Taxes from or in respect of any sum payable hereunder, the Guarantor will not reimburse the Government therefore, and:

(a) the Guarantor shall make such deductions; and

(b) the Guarantor shall pay the full amount deducted to the relevant taxation authority or other authority in accordance with applicable law; and within 30 days of any payment of Taxes, the Guarantor will furnish to the Government the original or a certified copy of a receipt evidencing payment thereof.

18. Successors and Assigns; Representatives. This Guarantee shall be binding upon the successors and assigns of the Guarantor, and shall inure to the benefit of the Government. The Guarantor may merge with or transfer substantially all of its assets to a successor guarantor. Such merger or transfer shall not require the consent of the Government. If the Guarantor is purchased by or merged with another entity, the Guarantor shall notify the Government of such purchase or merger within thirty (30) days thereof and the successor entity to the Guarantor shall deliver to the Government a written instrument unconditionally assuming and agreeing to perform all of the Guarantor's Obligations under this Guarantee.

19. Governing Law. This Guarantee shall be governed by, and construed and interpreted in accordance with, the federal laws of the United States of America, only to the extent that no federal law applies, then the laws of the State of New York shall apply.

20. Partial Invalidity. If any provision of this Guarantee or the application thereof to any Person or circumstance shall to any extent be held void, unenforceable, or invalid, then the remainder of this Guarantee or the application of such provision to Persons or circumstances other than those as to which it is held void, unenforceable, or invalid shall not be affected thereby and each provision of this Guarantee shall be valid and enforced to the fullest extent permitted by law.

[SIGNATURE BLOCK]

Table of Contents

K Representations and Certifications

K.1 On-Line Certifications

Federal Acquisition Regulation (FAR) 4.12, Representations and Certifications, requires Offerors to submit representations and certifications electronic annual representations and certifications via the System for Award Management (SAM) accessed via https://www.acquisition.gov, as a part of required registration (see FAR 4.1102). Offerors should also keep in mind that SAM-completed representations and certifications are considered part of the Offeror's proposal submission. Any changes to these representations and certifications would also be considered a change to your proposal submission and shall be in accordance with FAR Part 15. Your proposal MUST include your tax identification number (TIN) and Dun & Bradstreet number (DUNS).

Prospective contractors shall update the representations and certifications submitted to SAM as necessary, but at least annually, to ensure they are kept current, accurate, and complete. The representations and certifications are effective until one year from date of submission or update to SAM.

K.2 FAR 52.252-1 – Solicitation Provisions Incorporated by Reference (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at these addresses:

Federal Acquisition Regulation (FAR) Clauses: https://www.acquisition.gov/?q=browsefar

Table 1 FAR Clauses Incorporated by Reference

Clause	Title	Date
52.204-19	Incorporation by Reference of Representations and Certifications.	DEC 2014
52.225-25	Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran—Representation and Certification	DEC 2012

Department of the Interior Acquisition Regulation (DIAR) Clauses: http://farsite.hill.af.mil/vfdiara.htm

K.3 Department of Commerce Acquisition Regulation (CAR)

The contract clauses set forth in the following paragraphs of the Department of Commerce Acquisition Regulation (CAR) are incorporated in this contract (marked "X" when applicable) with the same force and effect as though set forth herein in full text. The designated clauses are incorporated as they appear in the DIAR on the date of this contract, notwithstanding the date referenced.

CAR Clauses: http://farsite.hill.af.mil/vfcara.htm

Table 2 CAR Clauses

Clause	Title	Date
1352.246-70	Place of Acceptance	APR 2010

K.4 FAR Clauses and/or Provisions in Full Text

K.4.1 Prohibition on Conducting Restricted Business Operations in Sudan--Certification (AUG 2009) – In accordance with FAR Part 25.702:

(a) *Definitions.* As used in this provision—

"Business operations" means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

"Marginalized populations of Sudan" means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and

(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

"Restricted business operations" means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

(b) *Certification*. By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(End of provision)

K.4.2 Prohibition on contracting with entities that engage in certain activities or transactions relating to Iran – In accordance with FAR 25.703:

(a) *Definitions*. As used in this section—

"Person"—

(1) Means—

(i) A natural person;

(ii) A corporation, business association, partnership, society, trust, financial institution, insurer, underwriter, guarantor, and any other business organization, any other nongovernmental entity, organization, or group, and any governmental entity operating as a business enterprise; and

(iii) Any successor to any entity described in paragraph (1)(ii) of this definition; and

(2) Does not include a government or governmental entity that is not operating as a business enterprise.

"Sensitive technology"—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

K.4.2.1 Iran Sanctions Act

(a) Certification.

(1) Certification relating to activities described in section 5 of the Iran Sanctions Act. As required by section 6(b)(1)(A) of the Iran Sanctions Act (50 U.S.C. 1701 note), unless an exception applies in accordance with paragraph (c) of this subsection, or a waiver is granted in accordance with 25.703-4, each offeror must certify that the offeror, and any person owned or controlled by the offeror, does not engage in any activity for which sanctions may be imposed under section 5 of the Iran Sanctions Act. Such activities, which are described in detail in section 5 of the Iran Sanctions Act, relate to the energy sector of Iran and development by Iran of weapons of mass destruction or other military capabilities.

(2) Certification relating to transactions with Iran's Revolutionary Guard Corps. As required by section 6(b)(1)(B) of the Iran Sanctions Act (50 U.S.C. 1701 note), unless an exception applies in

accordance with paragraph (c) of this subsection, or a waiver is granted in accordance with 25.703-4, each offeror must certify that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any significant transaction (i.e., a transaction that exceeds $3,500) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)(see OFAC's Specially Designated Nationals and Blocked Persons List at http://www.treasury.gov/ofac/downloads/t11sdn.pdf).

(b) Remedies. Upon the determination of a false certification under paragraph (a) of this subsection, the agency shall take one or more of the following actions:

(1) The contracting officer terminates the contract in accordance with procedures in part 49, or for commercial items, see 12.403.

(2) The suspending official suspends the contractor in accordance with the procedures in subpart 9.4.

(3) The debarring official debars the contractor for a period of at least two years in accordance with the procedures in subpart 9.4.

(c) Exception for trade agreements. The certification requirements of paragraph (a) of this subsection do not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see subpart 25.4).

K.4.2.2 Prohibition on contracting with entities that export sensitive technology to Iran

(a) The head of an executive agency may not enter into or extend a contract for the procurement of goods or services with a person that exports certain sensitive technology to Iran, as determined by the President and listed in the System for Award Management Exclusions via http://www.acquisition.gov (22 U.S.C. 8515).

(b) Each offeror must represent that it does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran.

(c) Exception for trade agreements. The representation requirement of paragraph (b) of this subsection does not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see subpart 25.4).

(End of provision)

K.4.3 52.204-8 Annual Representations and Certifications (Feb 2016)

(a)(1) The North American Industry Classification System (NAICS) code for this acquisition is 517210 Wireless Telecommunications Carriers.

(2) The small business size standard is 1,500 employees.

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b)(1) If the provision at 52.204-7, System for Award Management, is included in this solicitation, paragraph (d) of this provision applies.

(2) If the provision at 52.204-7 is not included in this solicitation, and the offeror is currently registered in the System for Award Management (SAM), and has completed the Representations and Certifications section of SAM electronically, the offeror may choose to use paragraph (d) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The offeror shall indicate which option applies by checking one of the following boxes:

□ (i) Paragraph (d) applies.

□ (ii) Paragraph (d) does not apply and the offeror has completed the individual representations and certifications in the solicitation.

(c)(1) The following representations or certifications in SAM are applicable to this solicitation as indicated: [None indicated]

(2) The following representations or certifications are applicable as indicated by the Contracting Officer:

__ (i) 52.204-17, Ownership or Control of Offeror.

__ (ii) 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products.

__ (iii) 52.222-48, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment- Certification.

__ (iv) 52.222-52, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Certification.

__ (v) 52.223-9, with its Alternate I, Estimate of Percentage of Recovered Material Content for EPA–Designated Products (Alternate I only).

__ (vi) 52.227-6, Royalty Information.

__ (A) Basic.

__(B) Alternate I.

__ (vii) 52.227-15, Representation of Limited Rights Data and Restricted Computer Software.

(d) The offeror has completed the annual representations and certifications electronically via the SAM website accessed through https://www.acquisition.gov. After reviewing the SAM database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in paragraph (c) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by clause number,

title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

FAR Clause # Title Date Change

_____ _____ _____ _____

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on SAM.

(End of provision)

K.4.4 52.227-15 Representation of Limited Rights Data and Restricted Computer Software (Dec 2007)

(a) This solicitation sets forth the Government's known delivery requirements for data (as defined in the clause at 52.227-14, Rights in Data--General). Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at 52.227-16, if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data--General clause at 52.227-14 included in this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.

(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and states [*offeror check appropriate block*]—

[ ] (1) None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or

[ ] (2) Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows:

_____

_____

_____

(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror.

(End of provision)

K.4.5 52.247-53 Freight Classification Description (APR 1984)

Offerors are requested to indicate below the full Uniform Freight Classification (rail) description, or the National Motor Freight Classification description applicable to the supplies, the same as offeror uses for commercial shipment. This description should include the packing of the commodity (box, crate, bundle, loose, setup, knocked down, compressed, unwrapped, etc.), the container material (fiberboard, wooden, etc.), unusual shipping dimensions, and other conditions affecting traffic descriptions. The Government will use these descriptions as well as other information available to determine the classification description most appropriate and advantageous to the Government. Offeror understands that shipments on any f.o.b. origin contract awarded, as a result of this solicitation, will be made in conformity with the shipping classification description specified by the Government, which may be different from the classification description furnished below.

For Freight Classification Purposes, Offeror Describes This Commodity as _____.

(End of Provision)

Table of Contents

List of Tables

List of Figures

L Instructions, Conditions, and Notices to Offerors or Respondents

L.1 FAR 52.252-1, Solicitation Provisions Incorporated by Reference (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer (CO) will make their full text available. The Offeror is cautioned that the listed provisions may include blocks that must be completed by the Offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the Offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this address: https://www.acquisition.gov/?q=browsefar.

Table 1 Solicitation Provisions Incorporated by Reference

Clause Number	Title	Date
52.204-6	Data Universal Numbering System (DUNS) Number	JUL 2013
52.204-7	System for Award Management	JUL 2013
52.214-34	Submission of Offers in the English Language	APR 1991
52.214-35	Submission of Offers in U.S. Currency	APR 1991
52.215-1	Instructions to Offerors – Competitive Acquisition	JAN 2004
52.216-29	Time-and-Materials/Labor-Hour Proposal Requirements – Non-Commercial Item Acquisition With Adequate Price Competition	FEB 2007
52.222-24	Preaward On-Site Equal Opportunity Compliance Evaluation	FEB 1999
52.222-46	Evaluation of Compensation for Professional Employees	FEB 1993
52.237-10	Identification of Uncompensated Overtime	MAR 2015

L.1.1 FAR 52.216-1, Type of Contract (APR 1984)

The anticipated contract resulting from the Request for Proposal (RFP) will be a single award Indefinite-Delivery-Indefinite-Quantity (IDIQ) with fixed price payments to the First Responder Network Authority (FirstNet) by the Contractor for each of the 56 states and territories resulting from this solicitation.

(End of Clause)

L.1.2 FAR 52.252-5, Authorized Deviations in Provisions (APR 1984)

The use in this solicitation of any Federal Acquisition Regulation (48 Code of Federal Regulations [CFR] Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

The use in this solicitation of any Department of the Interior (DOI) Acquisition Regulation (48 CFR Chapter 14) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

L.1.3 FAR 52.233-2, Service of Protest (SEP 2006)

Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the CO at the address below. A written, dated acknowledgement of receipt must be obtained. Address if mailed and/or hand carried:

Mr. Gregory Ruderman
U.S. Department of the Interior
Office of the Secretary, Interior Business Center
Acquisition Services Directorate
381 Elden Street, 4th Floor
Herndon, VA 20170

A copy of the protest served on the CO shall be simultaneously furnished by the protester to the Assistant Solicitor for Procurement and Patents, Office of the Solicitor, U.S. Department of the Interior, Room 6511, 1849 C Street, NW, Washington, DC 20240.

(End of Clause)

L.1.4 Independent Review of Protests to the Agency

Interested parties may request an independent review at a level above the CO of protests filed directly to the agency in accordance with Federal Acquisition Regulation (FAR) Part 33. This review is available as an alternative to consideration of the protest by the CO. Requests for independent review shall be submitted to the Chief of the acquisition office issuing the RFP, who will designate the official(s) to conduct the independent review.

L.1.5 Inquiries

Offerors are instructed to contact only the CO shown in Block 8 of Section A, Solicitation, Offer, and Award, for information about any aspect of this RFP. Prospective Offerors are cautioned against contacting government technical personnel in regard to this RFP prior to award of this procurement. If such a contact occurs and is found to be prejudicial to competing Offerors, the Offeror making such a contact may be excluded from further consideration for award.

Accordingly, all communications prior to award shall be directed to the CO named in Block 8 of Section A, Solicitation, Offer, and Award. Where possible, inquires shall be submitted in writing, email, or as otherwise instructed herein. Questions should be worded so as to avoid disclosing any potential proposed strategies or proprietary solutions. Questions and answers will be provided to all Offerors being solicited via the Federal Business Opportunities site (www.fbo.gov).

L.1.6 Incurring Costs

The CO is the only person who can legally obligate the Government for the expenditure of public funds. Costs shall not be incurred by recipients of this RFP in anticipation of receiving direct reimbursement from the Government. It is understood that your proposal will become part of the official file on this matter without obligation of the Government.

L.1.7 Involvement of Current and Former Government Employees

Awards to current Government employees or firms owned or controlled by them are restricted by FAR 3.601 to exceptional cases approved by the head of the contracting activity. Restrictions regarding current employees apply to regular employees and special Government employees (such as the FirstNet Board) as those terms are defined in 43 CFR Section 20.735-1, Definitions. To avoid an appearance of impropriety, preferential treatment, or unfair competitive advantage, the Government has established additional disclosure and review requirements for awards to or involving former Government employees.

The prospective Contractor shall provide a disclosure statement in its proposal identifying any current Government employees or former Government employees who will be involved in the proposal and/or resultant contract and the nature of their involvement or financial interests if:

- The Offeror is a current or a former Government employee.
- The Offeror is a business concern substantially owned or controlled by one or more current or former Government employees.
- The Offeror has employed in the preparation of this proposal or plans to employ on any contract resulting from this RFP a current or a former Government employee.

Disclosure requirements regarding former employees are limited to former regular and special Government employees whose employment terminated within two years prior to submission of this RFP. Involvement of such employees, either in preparing the proposal or under any resultant contract, is not necessarily precluded, but each case shall be reviewed against standards of conduct and procurement integrity restrictions on former employees.

L.1.8 Freedom of Information Act and Congressional Request

Offerors are apprised that information furnished under this RFP may not be subject to disclosure under the Freedom of Information Act (FOIA), under Section 821 of P.L. No. 104-201 (1997) in accordance with the Act.

Offerors should nevertheless be aware that proposals may be accessed through congressional request and are advised to clearly mark all items that are confidential to the business or contain trade secrets, proprietary information, or personal information. Marking of items will not necessarily preclude mandatory disclosure.

L.1.9 AQD Evaluation of Options Provision (OCT 2015)

The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic award. This solicitation notified Offerors that the award will include the Government's unilateral option to extend performance for an additional period up to six months under FAR 52.217-8, during which the pricing and terms of the period in which the option was exercised would apply. The Government cannot predict if or when the option may be exercised. Because any exercise of the Government's option extends the pricing and terms of the period in which the option was exercised, the Government expressly and affirmatively evaluates pricing for the option to extend under 52.217-8 co-extensive with the Government's price evaluation for each of the base and option periods of this award. Because pricing for each period subject to possible extension under the 52.217-8 has been evaluated, pricing for any possible future use of that option to extend has, likewise, been evaluated and would apply in strict accordance with this evaluation in the event of the Government’s exercise of the option to extend services.

(End of Provision)

L.1.10 1452.215-71, Use and Disclosure of Proposal Information (APR 1984)

(a) Definitions. For the purposes of this provision and the Freedom of Information Act (5 U.S.C. 552), the following terms shall have the meaning set forth below:

(1) "Trade Secret" means an unpatented, secret, commercially valuable plan, appliance, formula, or process, which is used for making, preparing, compounding, treating or processing articles or materials which are trade commodities.

(2) "Confidential commercial or financial information" means any business information (other than trade secrets) which is exempt from the mandatory disclosure requirement of the Freedom of Information Act, 5 U.S.C. 552. Exemptions from mandatory disclosure which may be applicable to business information contained in proposals include exemption (4), which covers "commercial and financial information obtained from a person and privileged or confidential," and exemption (9), which covers "geological and geophysical information, including maps, concerning wells."

(b) If the Offeror, or its subcontractor(s), believes that the proposal contains trade secrets or confidential commercial or financial information exempt from disclosure under the Freedom of Information Act, (5 U.S.C. 552), the cover page of each copy of the proposal shall be marked with the following legend:

> *"The information specifically identified on pages [to be completed by the Contractor] of this proposal constitutes trade secrets or confidential commercial and financial information which the Offeror believes to be exempt from disclosure under the Freedom of Information Act. The Offeror requests that this information not be disclosed to the public, except as may be required by law. The Offeror also requests that this information not be used in whole or part by the government for any purpose other than to evaluate the proposal, except that if a contract is awarded to the Offeror as a result of or in connection with the submission of the proposal, the Government shall have the right to use the information to the extent provided in the contract."*

(c) The Offeror shall also specifically identify trade secret information and confidential commercial and financial information on the pages of the proposal on which it appears and shall mark each such page with the following legend:

> *"This page contains trade secrets or confidential commercial and financial information which the Offeror believes to be exempt from disclosure under the Freedom of Information Act and which is subject to the legend contained on the cover page of this proposal."*

(d) Information in a proposal identified by an Offeror as trade secret information or confidential commercial and financial information shall be used by the Government only for the purpose of evaluating the proposal, except that (i) if a contract is awarded to the Offeror as a result of or in connection with submission of the proposal, the Government shall have the right to use the information as provided in the contract, and (ii) if the same information is obtained from another source without restriction it may be used without restriction.

(e) If a request under the Freedom of Information Act seeks access to information in a proposal identified as trade secret information or confidential commercial and financial information, full consideration will be given to the Offeror's view that the information constitutes trade secrets or confidential commercial or financial information. The Offeror will also be promptly notified of the

request and given an opportunity to provide additional evidence and argument in support of its position, unless administratively unfeasible to do so. If it is determined that information claimed by the Offeror to be trade secret information or confidential commercial or financial information is not exempt from disclosure under the Freedom of Information Act, the Offeror will be notified of this determination prior to disclosure of the information.

(f) The Government assumes no liability for the disclosure or use of information contained in a proposal if not marked in accordance with paragraphs (b) and (c) of this provision. If a request under the Freedom of Information Act is made for information in a proposal not marked in accordance with paragraphs (b) and (c) of this provision, the Offeror concerned shall be promptly notified of the request and given an opportunity to provide its position to the Government. However, failure of an Offeror to mark information contained in a proposal as trade secret information or confidential commercial or financial information will be treated by the Government as evidence that the information is not exempt from disclosure under the Freedom of Information Act, absent a showing that the failure to mark was due to unusual or extenuating circumstances, such as a showing that the Offeror had intended to mark, but that markings were omitted from the Offeror's proposal due to clerical error.

(End of provision)

L.2 General Instructions

Your proposal shall become the property of the Government and will not be returned. If your proposal contains information that you do not wish disclosed to the public or used by FirstNet for any purpose other than evaluation of your proposal, such restrictions shall be clearly indicated on each sheet containing such information (see FAR 52.215-1 listed in Table 1 Solicitation Provisions Incorporated by Reference).

Prior to submission of a proposal, the Offeror is expected to reach an understanding of the objectives of this RFP. If such a review establishes the need for correction or clarification, such information should immediately be brought to the attention of the CO, in accordance with the instructions contained herein, so that the matter can be resolved and, if necessary, official dissemination of such information can be made to all Offerors.

The Government reserves the right to request additional information as may be necessary to determine the Offeror’s qualifications for award or to clarify any aspects of the Offeror’s proposal. Such information shall be furnished promptly upon the Government’s request.

Offerors shall not be reimbursed for the costs of developing a proposal for this RFP.

One copy of each unsuccessful proposal will be retained in the contract file and all other copies will be destroyed. Additional copies of the successful proposal may be retained only as needed for contract administration and monitoring.

L.2.1 Partnering/Teaming List

As a courtesy, the Government has been compiling a list of those Offerors interested in subcontracting and teaming opportunities with other potential Offerors. If you are interested in being included on the list, please submit your business name and size and point of contact information (e.g., name, email address, phone number) no later than ***2:00 p.m. Eastern Time on Thursday, March 17, 2016***, to the

point of contact identified herein. All email inquiries shall have "Teaming List – RFP # D15PS00295" included in the subject line.

The partnering/teaming list is available via the Federal Business Opportunities (FBO) website (www.fbo.gov) and the FirstNet website (www.FirstNet.gov). Offerors are not required to be listed on the partnering/teaming list to submit a proposal. This is optional and solely intended to be a list of potential subcontracting and teaming opportunities. This list of potential subcontractors/teaming partners is not evaluated by the Government and, therefore, the Government accepts no liability for any resultant outcomes. Being placed on the list does not obligate the Government or any other party to make an award, subcontract award, or any other business opportunity.

L.2.2 Pre-Proposal Conference

The Government anticipates holding a pre-proposal conference and highly encourages Offerors to attend (in person or via webcast). However, attendance is not a prerequisite for submitting a proposal. The purpose of the pre-proposal conference is to provide potential Offerors the opportunity to further understand FirstNet's approach to the Nationwide Public Safety Broadband Network (NPSBN) and to ask questions, time permitting. At the Government's discretion, the Government will respond to RFP questions either verbally at the conference or in writing following the conference.

L.2.2.1 Pre-Proposal Conference Date, Time, and Location

Date	March 10, 2016
Time	From 1:30–5:00 p.m. Eastern Time
Registration Time	1:00 p.m. Eastern Time
Location	U.S. Geological Survey National Center Auditorium 12201 Sunrise Valley Drive Reston, VA 20192

L.2.2.2 Pre-Proposal Conference Attendance

Offerors may participate in the pre-proposal conference in person or remotely via webcast. Both the on-site event and the webcast will be free and open.

Pre-registration is required for on-site attendance as space may be limited. To pre-register, attendees shall send an email to FirstNetIndustryDay@firstnet.gov. On-site attendance is limited to three individuals from each company or organization. Registration is not required for the webcast.

On-site attendance will be on a first-come, first-served basis during pre-registration. Once the maximum number of attendees is reached, registration will close and subsequent requests for on-site participation will be denied. On March 10, 2016, pre-registered attendees will be required to check in on-site. Check-in will commence at 1:00 p.m. Eastern Time. Those who have not pre-registered will not be admitted.

In the event of any time and/or date changes to the pre-proposal conference, the Government will notify Offerors via an amendment to the RFP posted to FBO (www.fbo.gov).

L.2.2.3 Pre-Proposal Conference Questions and Answers

Offerors may ask questions at the pre-proposal conference or provide those questions in writing (via email) to the Government prior to the pre-proposal conference. These questions shall be submitted in

accordance with the instructions stated in Section L.2.3, Formal Communication – Requests for RFP Clarification.

The Government will only accept questions submitted by email utilizing the Questions Template in Section J, Attachment J-5; questions submitted by any other means, such as voicemail or fax will not be accepted. The Government will not attribute questions to the authors. This RFP may be amended as a result of the Government's response, and any amendments will govern over the posted questions/responses.

L.2.3 Formal Communication – Requests for RFP Clarification

The opportunity to submit all requests for RFP clarification begins upon the release of the RFP and ends no later than ***1:00 p.m. Eastern Time on Friday, February 12, 2016***. All requests for clarification shall be submitted in writing by email, as identified in Section J, Attachment J-5, Questions Template. The Offeror shall send requests for clarification to FirstNetRFPQuestions@firstnet.gov. All submissions shall reference this RFP number and title.

Requests transmitted via fax or phone will not be accepted.

Should any request for clarification be received after the date and time stated above, the Government reserves the right not to provide an answer. If, however, the Government determines the request for clarification addresses an issue of significant importance, the Government may provide a written response to all Offerors. Please note, questions and/or comments will not be protected by the Government as proprietary (see Section L.1.5, Inquiries).

Additionally, Offerors may determine or believe that the RFP package contains errors or omissions, or is otherwise unsound. In such cases, the Offeror shall immediately notify the CO in writing of such errors, omissions, or other issues in accordance with the instructions regarding submission of questions. The Offeror shall provide details and supporting rationale.

L.2.4 Submission of Capability Statements

As stated in Section M, Evaluation Factors for Award, Phase I of the multi-phased approach is submission of capability statements (see FAR Part 15.202). Interested parties should demonstrate they are qualified to perform the work by providing their capabilities as stated herein. The capability statement shall not exceed 50 pages in length (25 sheets of paper, double-sided print, 8.5" x 11" size paper) and shall be provided in Adobe PDF or Microsoft Word soft copy file format with Times New Roman font of 12 points or higher. Tables, charts, figures, and headers and footers may use a font size other than point 12 as long as it is legible. Any pages that exceed the 50-page limit will not be evaluated. The capability statement should provide information detailing:

- **Public safety use and adoption of the NPSBN** – Information demonstrating the Offeror's ability to successfully drive adoption and use of the NPSBN by public safety users.
- **Nationwide coverage and capacity** – Information demonstrating the Offeror's ability to provide Band 14 and non-Band 14 coverage and capacity in each of the 56 states and territories, including rural and non-rural areas.
- **Rural partnerships** – Information demonstrating the Offeror's existing and planned partnerships with rural telecommunications providers, including commercial mobile providers, utilizing existing infrastructure to the maximum extent economically desirable to speed deployment in rural areas.

- **Ability to monetize network capacity** – Information demonstrating the Offeror's strategy and demonstrating its ability to monetize network capacity, which may include a secondary user customer base and sales/distribution channels to reach primary and secondary users.
- **Financial sustainability** – Information demonstrating the Offeror's approach and financial sustainability. Additionally, information demonstrating its ability to develop, implement, sustain, and enhance the NPSBN based on the Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones set out in Section J, Attachment J-8, IOC/FOC Target Timeline.

The capability statement shall be received on or before ***2:00 p.m. Eastern Time on Thursday, March 31, 2016***. The capability statement shall be submitted in hard copy (one original and eight hard copies) and on three flash drives in Adobe PDF or Microsoft Word soft copy file format (to be submitted with the hard copies) to the addresses stated herein. In the event the hard copy and soft copy content conflict, the hard copy submission will take precedence over the soft copy version.

Please note it is the Offeror's responsibility to ensure/verify that the Government receives its submission on or before the date and time specified. If the capability statement is not received by the Government on or before the date and time specified, the Offeror's submission may be considered late.

The addresses designated for receipt of capability statements is:

ORIGINAL AND SEVEN (7) HARD COPIES AND TWO FLASH DRIVES TO:

Ms. Terrie L. Callahan
U.S. Department of the Interior
Office of the Secretary, Interior Business Center
Acquisition Services Directorate
381 Elden Street, 4th Floor
Herndon, VA 20170
Phone: 703-964-3596

ONE (1) HARD COPY AND ONE FLASH DRIVE TO:

Primary Points of Contact: Ms. Peggy O'Connor and Mr. Mouncef Belcaid
Alternate Point of Contact: Mr. Jordan Andrews and Mr. Michael Carroll
First Responder Network Authority
3122 Sterling Cir, Suite 100
Boulder, CO 80301

Phone: (303) 334-9660
Alternate Phone: (303) 334-9661

Please note that DOI locations are secured buildings. If offers are hand delivered, instruct the courier to check in at the guard desk and ask to call the point of contact identified above. A staff member will meet the courier to receive the submittal. All packages containing a capability statement shall be labeled and sealed as if for mailing, and the following information shall be marked on the outside:

- Capability statement for RFP number
- Date and time specified for receipt
- Name and address of the Offeror

- Name of the DOI/Interior Business Center (IBC) point of contact (Ms. Terrie L. Callahan in Herndon, VA) or the FirstNet points of contact (Ms. Peggy O'Connor and Mr. Mouncef Belcaid in Boulder, CO)

When submissions are hand carried or delivered by courier service or express delivery service (e.g., Federal Express, DHL), the Offeror assumes full responsibility for ensuring allocation of enough time to gain access to the IBC, Acquisition Services Directorate (AQD) staff in accordance with these instructions and to submit its capability statement by the time and date specified herein.

As stated above, please be advised that it is the Offeror's responsibility to ensure the Government receives its submission on or before the specified due date and time.

L.2.5 Submission of Proposals

Proposals shall be received ***on or before 2:00 p.m. Eastern Time on Tuesday, May 31, 2016***. Proposals shall be submitted in hard copy (one original and eighteen hard copies) and on two flash drives in Adobe PDF or Microsoft Word soft copy file format, with the exception of any Excel, map, and shape files, to be submitted with the hard copies. In the event the hard copy and soft copy content conflict, the hard copy version will take precedence over the soft copy version.

Please note it is the Offeror's responsibility to ensure/verify that the Government receives its submission on or before the date and time specified. If the proposal is not received by the Government on or before the date and time specified, the Offeror's submission may be considered late. Timeliness of receipt of any submission will be determined by the date and time received at the Reston, VA address shown herein.

The addresses designated for receipt of proposals is:

ORIGINAL AND THIRTEEN (13) HARD COPIES AND ONE FLASH DRIVE TO:

Mr. Gregory Ruderman (Department of the Interior, Acquisition Services Directorate)
U.S. Department of Commerce
First Responder Network Authority
12200 Sunrise Valley Drive, Suite 100
Reston, VA 20191-3402

Office Phone: (703) 964-3590

FIVE (5) HARD COPIES AND ONE FLASH DRIVE TO:

Primary Points of Contact: Ms. Peggy O'Connor and Mr. Mouncef Belcaid
Alternate Points of Contact: Mr. Jordan Andrews and Mr. Michael Carroll
First Responder Network Authority
3122 Sterling Cir, Suite 100
Boulder, CO 80301

Phone: (303) 334-9660
Alternate Phone: (303) 334-9661

Please note that these locations are secured buildings. If offers are hand delivered, instruct the courier to check in at the guard desk and ask to call the points of contact identified above. A staff member will meet the courier to receive the submittal. All packages containing proposal submissions shall be labeled and sealed as if for mailing, and the following information shall be marked on the outside:

- RFP number
- Date and time specified for receipt
- Name and address of the Offeror
- Name of the DOI/IBC point of contact (Mr. Gregory Ruderman in Reston, VA) or the FirstNet points of contact (Primary: Ms. Peggy O'Connor and Mr. Mouncef Belcaid or Alternate: Mr. Jordan Andrews and Mr. Michael Carroll in Boulder, CO)

When submissions are hand carried or delivered by courier service or express delivery service (e.g., Federal Express, DHL), the Offeror assumes full responsibility for ensuring allocation of enough time to gain access to the secure facility for submission delivery in accordance with these instructions and to submit its proposal by the time and date specified herein.

As stated above, please be advised that it is the Offeror's responsibility to ensure the Government receives its submission on or before the specified due date and time.

L.2.6 Assumptions, Conditions, and/or Exceptions

The Offerors shall submit, under a separate tab, ***in each volume identified herein***, all (if any) assumptions, conditions, or exceptions with any of the terms and conditions of this RFP. If not noted in its proposal, it will be assumed that the Offeror proposes no assumptions, conditions, or exceptions for award and agrees to comply with all of the terms and conditions as set forth herein. It is not the responsibility of the Government to seek out and identify assumptions, conditions, or exceptions buried within the Offeror's proposal.

For proposal preparation purposes, if there are any assumptions, conditions, or exceptions made pertaining to demarcation between the Government's responsibility and/or the Contractor, the Offeror shall describe the specific demarcation points and/or assumptions, conditions, or exceptions within the proposal submission.

L.3 Proposal Format and Submission Instructions

Proposals, signed by an official authorized to bind the Offeror, shall set forth full, accurate, and complete information as required by this RFP. The penalty for making false statements is prescribed in 18 U.S.C. § 1001. Failure to furnish full and complete information requested may cause an offer to be determined unacceptable, and it may be removed from consideration for award.

In responding to this RFP, the Offerors shall prepare and submit the indicated numbers of copies (see Section L.2.5, Submission of Proposals) and required information that constitutes the Offeror's complete proposal submission. Additionally, the Offeror's information and submission shall be organized by volume as indicated below. Each volume shall include an Executive Summary that shall not exceed 4 pages in length (2 sheets of paper, double-sided print); each Executive Summary must clearly identify what portions of the volume are provided in soft-copy format (as allowed in accordance with Section L) for verification and validation purposes. Specifically, the business management volume shall be separate from the technical and pricing volumes.

Any page limitation for each proposal volume is identified within that section. However, the following information applies to *each* volume. The volumes shall be provided in Adobe PDF or Microsoft Word soft copy file format. A page is defined as Times New Roman Font Size 12, single-spaced, 8.5" x 11" size paper with one (1) inch margins top, bottom, left, and right. Maps, required Section J spreadsheets pertaining to network statistics, and large graphics or diagrams in the business management and technical volumes may use 11" x 17" size paper, but will be counted as two pages per 11" x 17" foldout.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Tables, charts, figures, and headers and footers may use a font size other than point 12 as long as it is legible. The page limitation excludes the cover page; Executive Summary; Section A, Solicitation, Offer, and Award; signed acknowledgements; table of contents and listing of tables, drawings, and/or exhibits; small business subcontracting plan; past performance references; and financial resources as identified herein. The Government shall treat page limitations as maximums. If exceeded, the CO will remove the excess pages prior to evaluation. The Government will not read or evaluate removed pages.

The Government reserves the right to request Offerors to conduct oral presentations and/or technical demonstrations as a result of this RFP (see Section M, Evaluation Factors for Award, Section M.2, Evaluation Process).

Proposal submittals to the Government shall be in three (3) volumes: Business Management, Technical, and Pricing.

L.3.1 Volume I – Business Management

The business management volume contains all information needed to communicate to the Government that the Offeror has well-developed processes in place to ensure effective program management and disciplined fiscal processes as identified within this section. Additionally, the Offeror shall include a small business subcontracting plan, Contractor responsibility information, and information on past performance in this volume.

The business management proposal shall not exceed 200 pages in length (100 sheets of paper, double-sided print). This page count excludes those items identified in Section L.3.1.1, Section One – General; the Solicitation Conformance Traceability Matrix; the Small Business Subcontracting Plan; Past Performance reference forms; the resumes, Integrated Master Schedule, and Work Breakdown Structure (WBS) referenced in L.3.1.2, Section Two – Leadership and Program Management; the Public Safety Device Connections Template and Section J, Attachment J-23, End User Pricing Tables, referenced in L.3.1.3, Section Three – Public Safety Customer Acquisition; Quality Assurance Surveillance Plan (QASP) reference in Section L.3.1.4, Section Four – Customer Care and Life-Cycle Sustainment; all items identified in Section L.3.1.5, Section Five – Offeror Financial Sustainability; and the executed Parental Guarantee Agreement identified in Section J, Attachment J-27. The business management proposal shall contain the following information and be broken down in the following sections.

L.3.1.1 Section One – General

The Offeror shall complete blocks 13, 15, 16, and 18 of Section A, Solicitation, Offer, and Award, and sign block 17 to show that the Offeror has read and agrees to comply with all the terms, conditions and instructions provided in the RFP unless otherwise noted in the assumptions, conditions, or exceptions section pertaining to the proposed solution. If there are any amendments to the RFP, the Offeror shall complete block 14 of Section A, Solicitation, Offer, and Award, and include a signed acknowledgement for all RFP amendments.

The Offeror shall describe its corporate management structure as well as the structure of the proposed team and the relationship between these organizations and all subcontractors proposed to perform all aspects of the objectives (as defined by the Offeror). Indicate the date the contracting entity was organized and indicate whether the organization is a separate entity, a division, or subsidiary

corporation. If it is a division or subsidiary corporation, provide the name and address of the parent company. Include your Taxpayer Identification Number (TIN) and DUNS number.

This volume shall also contain a section that includes a statement of intention to comply with the objectives stated herein and a statement of intention to comply with all terms and conditions of the contract unless otherwise noted in the assumptions, conditions, or exceptions section pertaining to the proposed solution.

As part of Volume I, Business Management, the Offeror shall propose a Performance Work Statement (PWS) identifying the tasks required for the deployment and operation of the NPSBN. The PWS shall address the objectives specified in Section C, Statement of Objectives (SOO) and the associated attachments in Section J. The PWS, evaluated to be the best overall solution, will replace the SOO in the subsequent contract.

Volume I, Business Management, shall also include separate tabs noting the solution for each Day 1 task order identified in Section B, Supplies or Services and Prices/Costs, Section B.2.1, Day 1 Task Orders. Each separate tab noting the solution for each Day 1 task order shall not exceed 50 pages in length (25 sheets of paper, double-sided print).

L.3.1.1.1 Solicitation Conformance Traceability Matrix

The Offeror shall fill out the Solicitation Conformance Traceability Matrix (SCTM)—available in Section J, Attachment J-22, SCTM—indicating the proposal reference information as it relates to the documents included in the RFP. If this matrix conflicts with any other requirement, direction, or provision of this RFP, the other reference and RFP information will take precedence over the Contractor-completed SCTM.

L.3.1.1.2 Small Business Subcontracting Plan Requirements

Offerors that qualify as large businesses shall submit a small business subcontracting plan following the guidelines identified in FAR 52.219-9, Small Business Subcontracting Plan (OCT 2015).

The plan submitted under this RFP shall comply with the format contained in Section J, Attachment J-26, Sample Small Business Subcontracting Plan.

The CO will make an affirmative determination regarding the acceptability of the small business subcontracting plan as one of the elements in determining eligibility for award.

Offerors that intend to use a subcontractor in performance of this contract shall provide evidence of the proposed subcontractor's commitment. If proposing a joint venture, the Offeror shall provide a copy of the joint venture plan/agreement. The Offeror shall describe how small business participation will contribute to its overall comprehensive subcontracting goals. The Offeror shall describe specific efforts to ensure the resulting contract meets or exceeds proposed small business subcontracting goals.

The requirements of clause FAR 52.219-9 and this provision do not apply when 1) the Offeror is a small business; 2) the work is to be performed entirely outside of any state, territory, or possession of the United States; the District of Columbia; and the Commonwealth of Puerto Rico; or 3) the contract, including all future modifications, will not exceed $700,000. The requirement may also be waived if the CO determines that the resultant contract does not offer subcontracting opportunities.

L.3.1.1.3 Contractor Responsibility Information

The Offeror shall provide information demonstrating that it is responsible within the meaning of FAR 9.104-1. In addition to the general responsibility standards in FAR 9.104-1, there is a special

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

responsibility standard that applies to this solicitation. This standard applies to all Offerors. In order to be determined responsible on this solicitation, an Offeror shall demonstrate expertise needed for adequate contract performance. The Offeror shall present evidence that it (1) has experience in efficiently managing complex engineering, development, and operational activities; (2) has experience in rapidly designing, deploying, operating, and optimizing state-of-the-art communications networks; and (3) has ready access to and experience in attracting and retaining appropriate talent.

L.3.1.1.4 Past Performance

The Offeror shall provide three (3) references of same and/or similar efforts performed by the Offeror and/or any/all subcontractors and/or teaming partners within the last three years. Each reference shall include the following information:

- Project title
- Description of the project
- Contract number (if applicable)
- Government agency/non-Government organization
- Contracting Officer's Representative/contract point of contact's name, address, email address, and phone number
- CO/contract point of contact's name, address, email address, and phone number
- Current status, i.e., completed (start and end dates) or in progress (start and estimated completion dates)
- Dollar value and type of contract
- Key personnel (highlight those individuals who worked on the relevant project and are being proposed for this effort)

The Offeror shall detail existing 3rd Generation Partnership Program (3GPP) standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its subcontractors and/or teaming partners. This would include additional details of existing public safety networks and infrastructure operated, controlled, or managed by the Offeror or its partners.

Refer to Section J, Attachment J-25, Past Performance Reference Information Form, for a sample format. If you believe the Government may find derogatory information as a result of checking your past performance record, please provide an explanation and any remedial action taken by your organization to address the problem(s).

In the case where an Offeror does not have any relevant past performance and/or experience related to the objectives identified in Section C, SOO, it shall provide an explanation in the Past Performance section of the Business Management volume. The Government may also consider information obtained through other sources. For Offerors with no relevant past performance, the Government may take into account information regarding the past performance of personnel with relevant past performance or subcontractors that will perform key aspects of this contract.

The Past Performance section of the Business Management volume may address any other topics considered pertinent to a demonstration of the Offeror's knowledge, competence, and capability to perform this contract.

L.3.1.1.5 Offeror's Experience

Describe the Offeror's experience as it relates to the overall proposed solution for the NPSBN. This shall include the structure and experience of the proposed subcontractors/teaming partners, and the relationship between these organizations proposed to perform major or critical aspects of the NPSBN (as defined by the Offeror) shall be listed. If there are any items stated in Section L.3.1.1.4, Past Performance, that are also applicable to the Offeror's current experience, these shall be addressed in this section. Specifically, the Offeror shall detail current 3GPP standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its subcontractors and/or teaming partners. This would include additional details of existing public safety networks and infrastructure operated, controlled, or managed by the Offeror or its partners.

L.3.1.2 Section Two – Leadership and Program Management

To demonstrate its expertise in leadership and program management, the Offeror shall:

- Provide a management plan that describes the proposed approach to meet the objectives as defined in Section C, SOO, and associated attachments in Section J. This shall include but is not limited to a corporate-level organizational structure with charts to identify the size, scope, and structure of the Offeror's entity; a comprehensive program management approach reflecting the Offeror's ability to provide seamless and efficient management of the NPSBN for the life of the contract; a change management approach, including relevant processes and procedures; the proposed approach for managing the contract at the corporate, contract, and task order levels; the proposed approach for supporting and facilitating FirstNet's compliance with the Act and other applicable laws; and proposed escalation and resolution procedures, including planned integration and coordination with FirstNet personnel.
- Provide a staffing plan that includes but is not limited to the Offeror's proposed organizational structure for leadership of the NPSBN; identify staffing, including roles and responsibilities as well as resumes, for key personnel and executive leaders who will support FirstNet.
- Provide an Integrated Master Schedule and WBS that addresses all build-out and transition-to-operations activities. The Offeror shall note, in the WBS, those tasks that include deliverables. The Offeror shall identify, in the WBS, the tasks required for the deployment and the operation of the NPSBN such that the objectives (specified in Section C, SOO, and the associated attachments in Section J) are met at the task and subtask level. The Offeror shall propose a milestone timeline detailing its solution in accordance with the IOC/FOC milestones contained in Section J, Attachment J-8, IOC/FOC Target Timeline.
- Provide details of existing 3GPP standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its proposed teaming partners and/or subcontractors.
- Describe how the solution leverages existing commercial and/or other infrastructure.

L.3.1.3 Section Three – Public Safety Customer Acquisition

To demonstrate its ability to acquire and retain public safety customers, the Offeror shall, at a minimum:

- Complete the Public Safety Device Connections Template (Section J, Attachment J-24, PS Device Connections tab), detailing the Offeror's anticipated number of public safety device connections for the primary user group, which consists of law enforcement, fire, and emergency medical

services users, as well as the extended primary user group, which consists of all other public safety users, as defined in the Act. The number of connections shall be broken out by each of the 56 states and territories over the life of the IDIQ contract. For proposal planning and evaluation purposes, the Offeror shall assume that connection targets start from the

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

estimated task order date (as defined in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders). For example, year 1 of the Public Safety Device Connections Template (Section J, Attachment J-24, PS Device Connections tab) corresponds with the first year of the task order award. Actual state and territory task order awards will trigger the IOC/FOC milestones (Section J, Attachment J-8, IOC/FOC Target Timeline) and the disincentive mechanism as detailed in the QASP (Section J, Attachment J-6, Quality Assurance Surveillance Plan). Connections proposed by the Offeror, beyond the IDIQ period of performance, will not be subject to the disincentive mechanism detailed in the QASP (Section J, Attachment J-6, Quality Assurance Surveillance Plan).

- FirstNet has aggregated stakeholder data to produce a nationwide view that estimates the current subscriber and device demand at a state level for the primary user group, which consists of law enforcement, fire, and emergency medical services users, as well as the extended primary user group, which consists of all other public safety users, as defined in the Act. This information can be found in the Public Safety Device Connections Template (Section J, Attachment J-24) in the Users_Devices_By State worksheet and can be used as a reference by the Offeror when detailing the Offeror's anticipated number of public safety device connections. The estimates were developed based on input from states, territories, tribal nations, and federal agencies, as well as FirstNet estimates.
- Describe the Offeror's approach to sales and marketing to public safety within the context of its greater corporate strategy.
- Identify the go-to-market strategy and sales channels to be used by the marketing and sales organization(s) in offering, selling, and marketing services to public safety users. Channels may include but are not limited to direct, indirect, third party, Internet, telemarketing, and strategic alliances.
- Describe a strategy to collaborate with public safety stakeholders, associations, and other pertinent organizations, such as the Association of Public-Safety Communications Officials, National Association of State Chief Information Officers, International Association of Chiefs of Police, and Public Safety Advisory Committee.
- Describe public safety end-user pricing strategies for all products, services, and devices. These strategies shall include details on priority and preemption for public safety as well as public safety services for both post-paid and pre-paid service offerings on Band 14 and non-Band 14 networks. Complete the tables in Section J, Attachment J-23, End-User Pricing Tables, which represent indicative pricing and service plans available to public safety users. When completing the tables, include any assumptions, as instructed herein, used in determining indicative pricing—such as details on usage caps, roaming caps, throttling, and contract length—and describe any proposed volume discount schedule and special pricing mechanisms to support public safety adoption and use of the NPSBN.
- Describe the Customer Relationship Management (CRM) systems and tools that will be used in support of selling FirstNet devices and services and how the Offeror will report on related Key Performance Indicators (KPIs).
- Describe the form and functionality of a FirstNet-branded, customer-facing Web-based portal that will enable public safety users, including individually liable and enterprise-liable customers, to view and order, among others, devices, service offerings, and accessories.
- Describe the approach to foster a vibrant applications ecosystem. This shall include but is not limited to:
    - A strategy to market the FirstNet applications store and target public safety users

  - A description and details of current or planned agreements and contracts with providers of software applications applicable to the public safety market
  - Marketing strategies that will be implemented to attract and work with developers for public safety applications development
  - Social media platforms to engage the public safety community
- Describe details of its sales and marketing structure, particularly sales and marketing channels specific to public safety, and if no channels specific to public safety, describe plans for developing or leveraging such channels. Describe the marketing and sales organization(s) tasked with supporting FirstNet, including but not limited to the organization's function, size, structure, geographic distribution (e.g., whether resources are based in the United States; the location and number of employees/subcontractors located outside of the United States), and relation to the Offeror (e.g., direct, indirect, outsourced). Additionally, describe the proposed approach to ensure strategic alignment and mitigation of sales and marketing channel conflict among teaming partners to ensure adoption and use of the NPSBN.
- Describe how the proposed solution will meet current, emerging, and future public safety needs, requirements, and standards. Explain how the services, devices, and applications ecosystems will evolve over the life of the contract; how the proposed services tie back to a network deployment plan; and when services will be generally available. Additionally, provide a roadmap of the existing and future Band 14 products, services, and devices to be offered and describe how new services and features will incentivize use of the NPSBN. Complete Table 3 in Section J, Attachment J-23, End-User Pricing Tables, to identify the anticipated supplier and estimated price points for Band 14-enabled devices for public safety.

L.3.1.4 Section Four – Customer Care and Life-Cycle Sustainment

The Offeror shall provide the following information regarding public safety service delivery, including all linkages to sales, marketing, fulfillment, customer care, and other relevant functions:

- Describe how the metrics proposed and outlined in the Offeror's proposed Quality Assurance Surveillance Plan (QASP) will be used to monitor and manage the service delivery system—including activation, repair, technical assistance, replacement devices, and emergency restoration—and customer satisfaction over the life of the contract.
- Describe the Offeror's proposed customer care strategy, which shall address:
  - How the Offeror will minimize churn and promote customer retention among public safety users.
  - How an integrated customer care model will be delivered for public safety users.
  - The customer care organization(s) that will support the NPSBN, including the organization's function, size, structure, geographic distribution (e.g., whether resources are based in the United States; the location and number of employees/subcontractors located outside of the United States), and relation to the Offeror (i.e., in-house, contracted out).
  - The proposed solution for resolving customer service requests or issues with service delivery or products.
  - How the Offeror will provide responsive corrective action for service impairments and service restoral when the action involves direct contact with the customer.
  - How the Offeror will train the customer on device or service usage.

- The proposed strategies for recruitment and retention of the customer care workforce, including how to train staff on existing and emerging products, services, and applications.
- Customer care systems and tools that will be used in support of public safety customer care.

- Detail the proposed comprehensive billing management strategy for public safety. The strategy shall include but is not limited to descriptions of the current billing support services for broadband services, wireless services, and, if applicable, public safety services; the billing support service delivery for the NPSBN; customized billing available for state, local, and tribal agencies using the NPSBN; and the Offeror's approach to billing throughout the FirstNet service area, including proposed roaming charges.

L.3.1.5 Section Five – Offeror Financial Sustainability

To allow the Government to assess if the Offeror has the financial sustainability to develop, implement, sustain, and enhance the NPSBN in accordance with the time frames, duration, and objectives set out in this RFP, the Offeror shall provide the financial information listed below. If the Offeror represents a consortium, partnership, or any other form of a joint venture, appropriate information shall be provided for all such entities comprising the Offeror.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

L.3.1.5.1 Financial Resources

The Offeror shall provide, at a minimum, copies of the following financial information, with the exception of the financial statements identified below. If the entity for which financial statements are submitted files reports with the U.S. Securities and Exchange Commission (SEC), the Offeror may provide electronic links to the most recently filed SEC Forms 10-K, 10-Q, and Form 8-K for all such reporting entities in lieu of hard copy submissions. If the Offeror is a newly formed entity, expressly state that it is or will be a newly formed entity and does not have independent financial information at the time of response to the RFP. If the Offeror is a newly formed entity, it must provide the following financial information for the parent or guarantor entity(ies), which will guarantee the Offeror's obligations under the contract and allow the Government to evaluate financial resources.

- **Financial Statements** – Provide the financial statements and accompanying information listed below. Financial statements shall be prepared in accordance with U.S. Generally Accepted Accounting Principles. Information in the balance sheets, income statements, and statements of cash flow shall be provided in U.S. Dollars. If the entity for which financial statements are submitted files reports with the U.S. Securities and Exchange Commission (SEC), the Offeror shall provide electronic links to the most recently filed SEC Forms 10-K, 10-Q, and Form 8-K for all such reporting entities.
    - **Audited Financial Statements** – Provide audited financial statements for the last three years for the Offeror. The Offeror's fiscal year-end financial statements shall be audited by an independent party qualified to render audit opinions (i.e., certified public accountant). If audited financials are not available, include unaudited financial statements for the entity, certified as true, correct, and accurate by the chief executive officer, the chief financial officer, treasurer, or other authorized signatory (the "Financial Officer") of the entity. Financial statement information shall include the following information:
        - Opinion letter (auditor's report)
        - Balance sheet
        - Income statement
        - Statement of cash flow
        - Footnotes
    - **Interim Unaudited Financial Statements** – In addition to the audited financial statements, provide interim unaudited statements for the above entities. These statements shall reflect the most recent completed fiscal year or the period since the most recent completed fiscal year and shall include the following information:
        - Balance sheet
        - Income statement
        - Statement of cash flow
- **Credit Ratings** – Provide the most recent credit rating(s), if any, associated with the Offeror. If no credit ratings exist, include a statement specifying that no credit ratings exist.
- **Material Changes in Financial Condition** – Provide a letter from the chief financial officer for the Offeror, either (1) providing information on any material changes in the Offeror's financial condition since the date of the last audited financial statement and those that are pending or (2) certifying that no such material changes have occurred. In instances where a material change has occurred or is anticipated, provide a statement describing each material change in detail, the likelihood that developments will continue during the period of performance of the

contract, and the projected full extent of the changes likely to be experienced in the periods ahead. Estimates of the impact on revenues, expenses, and the change in equity shall be provided separately for each material change as certified by the chief financial officer. References to the notes in the financial statements are not sufficient to discuss the impact of

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

material changes. Discuss measures that would be undertaken to insulate FirstNet from any recent material adverse changes, as well as those currently in progress or reasonably anticipated in the future. The following list identifies items that the Government would consider a material change in financial condition. This list is intended to be indicative only and not exhaustive.

- An event of default or bankruptcy involving the affected entity, parent corporation of the affected entity, or any controlled subsidiary or affiliate
- A change in tangible net worth of 10 percent of shareholder equity
- A sale, merger, or acquisition exceeding 10 percent of the value of shareholder equity prior to the sale, merger, or acquisition that in any way involves the affected entity, parent corporation, or financially responsible party of the affected entity
- Adverse changes in credit rating for the affected entity or parent corporation of the affected entity
- Inability to meet material conditions of loan or debt covenants by the affected entity or parent corporation of the affected entity, resulting in the need for a waiver or modification of agreed financial ratios, coverage factors or other loan stipulations, or additional credit support from shareholders or other third parties
- In the current and three most recently completed Offeror fiscal years, the affected entity or the parent corporation of the affected entity (1) incurs a net operating loss; (2) sustains charges exceeding 5 percent of the then shareholder equity due to claims, changes in accounting, write-offs, or business restructuring; (3) implements a restructuring/reduction in labor force exceeding 200 positions; or (4) involves asset disposition exceeding 10 percent of the then shareholder equity
- Other events known to the affected entity that represent a material change in the financial condition over the past three years or that may be pending for the next reporting period (e.g., pending litigation)

L.3.1.5.2 Sources of Funding and Financing

The Offeror shall detail each source of funding or financing used to support the build-out or operation and maintenance of the NPSBN, including the costs, rights, and obligations of each type of funding or financing and details of agreements with funding/financing entities.

L.3.1.5.3 Parent Company Guarantees

The Offeror shall provide details (including terms and conditions) of a guarantee (or equivalent security) from an entity of sufficient financial standing to meet the Offeror's obligations, including disincentive payments, throughout the life of the contract, in the form of a Parental Guarantee Agreement. The Offeror shall submit a fully executed Parental Guarantee Agreement (see Section J, Attachment J-27, Parental Guarantee Agreement) signed by an official authorized to bind the Offeror and the proposed Parental Guarantor. This executed Agreement shall be submitted in Volume I – Business Management, as identified in Section L.3.1.

L.3.1.5.4 Commercialization of Excess Network Capacity

The Offeror shall provide a detailed approach reflecting how the Offeror plans to use Band 14 in its business model, including plans to commercialize the 20 MHz of Band 14 network capacity beyond its sales channel(s) for public safety.

L.3.1.6 Section Six – Delivery Mechanism for State Plans

The Offeror shall provide a clear written description of a Web interface tool for sharing information with governors and/or state decision makers. FirstNet's objectives for the online delivery mechanism are

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

described in Section J, Attachment J-18, Delivery Mechanism Objectives for State Plans. The Offeror's description of the tools shall include:

- The capabilities, functionality, and information sharing methodology for each type of stakeholder (state, enterprise, and individual)
- How to navigate the online system
- The access control methodology, security, and authentication approach for managing information
- A graphical representation of content provided with the Offeror's proposal relevant to state planning (e.g., coverage maps, device portfolio, service plans)
- The methodology for incorporating additional data or new information in each section of the online system

If the Government determines a demonstration of the online tool is required, additional details will be provided at a later date.

L.3.1.7 Section Seven – Quality Assurance Surveillance Plan

The Offeror shall provide a QASP, in accordance with Section J, Attachment J-6, which defines what FirstNet and the Contractor must do to ensure that the Contractor has performed in accordance with the performance metrics/standards as agreed upon in the contract. Additionally, the QASP is intended to provide a plan to assess the performance of the Contractor in meeting the program's SOO. The Contractor is responsible for management and quality control actions to meet the terms of the contract. The proposed plan shall leverage industry best practices, technology enhancements, and professional expertise. The plan shall employ standard business practices and processes and minimize risk while improving quality of service.

The QASP shall include, at a minimum, a surveillance schedule and clearly state the surveillance method(s) to be used. The QASP must address how the Contractor will measure, assess, manage, and report on the quality of its performance.

L.3.1.8 Section Eight – Deliverables Table

The Offeror shall complete Section J, Attachment J-16, Deliverables Table, noting the deliverables that Offeror will provide following award. The proposed deliverables shall reflect industry best practices and professional expertise. The deliverables shall align with the proposed performance metrics/standards defined in the Offeror's QASP (Section J, Attachment J-9, QASP Surveillance Matrix Template). The proposed deliverables for the successful solution will be incorporated into the final Deliverables Table attached to the contract. The Deliverables Table is a "living document," and the Government may review and revise it on a quarterly basis in coordination with the Contractor.

In addition to any Contractor-proposed deliverables, FirstNet requires specific deliverables to monitor performance and demonstrate value. Those deliverables, which are identified in Section F, Deliverables and Performance, Section F.4.2, FirstNet-Required Deliverables, shall be included in the Offeror's proposed Deliverables Table.

L.3.2 Volume II – Technical

The technical volume shall demonstrate the Offeror has a thorough understanding of coverage and capacity, products, and architecture as they relate to the objectives identified within Section C, SOO, and the associated attachments contained in Section J.

The technical proposal shall not exceed 300 pages in length (150 sheets of paper, double-sided print); this excludes coverage maps and the following Section J attachments from the page limitation: Section J, Attachment J-11, Device Specifications Template; Section J, Attachment J-12, Test Strategy Template; and Section J, Attachment J-17, Coverage and Capacity Template. Section J, Attachment J-17, Coverage and Capacity Template, may be submitted in a soft copy format only as stated herein (flash drive). The technical proposal shall contain the following information and be broken down by the following sections.

L.3.2.1 Coverage and Capacity

The Offeror shall provide a clear, concise description regarding its proposed approach in deploying a network to implement coverage and capacity. This shall include:

- Coverage and Capacity Maps and Statistics
- Radio Access Network (RAN) Solutions and Strategy
- IOC/FOC Milestones for Coverage and Capacity

The proposed solution for coverage and capacity shall address the elements described below according to the IOC/FOC target timeline detailed in Section J, Attachment J-8. Maps submitted by the Offeror shall be based on a bin size no greater than 30 x 30 meters, include Esri shapefiles and MapInfo files (in electronic format), and reference the information contained in Section J, Attachment J-1, Coverage and Capacity Definitions. The statistics shall utilize Section J, Attachment J-17, Coverage and Capacity Template.

The Offeror must complete Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, to demonstrate its ability to meet the objective to provide coverage in all states and territories and to ensure that rural coverage includes partnerships with rural telecommunications providers. The Offeror shall note whether both Band 14 and non-Band 14 coverage are included in each of the 56 states and territories (yes/no), as well as list current and planned partnerships with rural telecommunications providers by state/territory. Lastly, Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, requests tabulation, by state, of the percentage of rural coverage achieved via partnerships with rural telecommunications providers. The Offeror's solution must demonstrate intent to exercise rural telecommunications provider partnerships for at least 15 percent of the total persistent rural coverage nationwide. In the case of anticipated but unexecuted agreements, the Offeror should describe its strategy to mitigate any risks or impediments that may arise should the agreements not come to fruition. While Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, requests these data by states, the 15 percent coverage factor will be evaluated on a nationwide basis only as stated in Section M, Evaluation Factors for Award.

L.3.2.1.1 Coverage and Capacity Maps and Statistics

The Offeror shall submit all applicable information as defined in Table 2 Coverage Maps Required for Coverage and Capacity. The Offeror shall submit all network statistics, as defined in Table 3 Network Statistics Required for Coverage and Capacity, for each of the 56 states and territories in the Coverage and Capacity Template (Section J, Attachment J-17). The Offeror shall refer to the guidelines provided in Section J, Attachment J-1, Coverage and Capacity Definitions. The Offeror shall describe the details for the network planning design as stated in Section L.3.2.1.2.2, Network Planning and Design, below and the methodologies used to create coverage maps and associated capacity information.

Table 2 Coverage Maps Required for Coverage and Capacity

Level	Band	Phase	Maps Required	Format	Submittal Method
Nationwide	Non-Band 14	FOC	One (1) nationwide map of each file format, depicting coverage by technology: Long Term Evolution (LTE), 3G, 2G, and roaming layers	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via Secure File Transfer (SFT) with Offeror-provided credentials or Offeror-provided portable drive
Nationwide	Band 14	FOC	One (1) nationwide map of each file format, depicting the LTE analysis layers specified in Section L.3.2.1.1.6	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive

* Note: If needed, the Offeror may provide multiple regional MapInfo & Esri (.shp) files that display coverage for smaller areas versus for the entire nation to fit within application and file size limitations. If regional maps are provided, they shall collectively represent nationwide coverage.

The Offeror shall provide the following network statistics in the Section J, Attachment J-17, Coverage and Capacity Template.

Table 3 Network Statistics Required for Coverage and Capacity

Coverage Type	Level	Phase
Non-Band 14 Area Covered **	State/Territory	FOC
Non-Band 14 Population Covered **	State/Territory	FOC
Band 14 Area Covered	State/Territory	FOC
Band 14 Population Covered	State/Territory	FOC
Band 14 Network Capacity	County	FOC

** Note: Non-Band 14 coverage statistics shall be broken down by technology: LTE, 3G, 2G, and roaming.

L.3.2.1.1.1 Non-Band 14 Area Coverage

The Offeror may propose persistent coverage using non-Band 14 frequencies. This may include all or some of the following technologies, depending on the Offeror's proposal: LTE, 3G, 2G, and any roaming via the Offeror's partners. If proposed, the Offeror shall provide a breakdown of offered non-Band 14 coverage, including (as described in Table 2 Coverage Maps Required for Coverage and Capacity) and network statistics (as described in Table 3 Network Statistics Required for Coverage and Capacity), for each proposed technology.

L.3.2.1.1.2 Non-Band 14 Population Coverage

The Offeror may propose persistent population coverage using non-Band 14 frequencies. The Offeror shall overlay its proposed non-Band 14 area coverage map (including the technology layers) with the FirstNet-provided 2010 U.S. Census 1 mile by 1 mile population count map (see Section J, Attachment J-1, Coverage and Capacity Definitions) and provide the proposed output population coverage statistics

(by state/territory) using the Section J, Attachment J-17, Coverage and Capacity Template. Non-Band 14 population coverage may include the following technologies, depending on the Offeror's proposal: LTE,

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

3G, 2G, and roaming (via the Offeror's partners). The Offeror shall provide a breakdown of offered population coverage, including coverage maps and network statistics, for each proposed technology.

L.3.2.1.1.3 Band 14 Area Coverage

The Offeror shall propose persistent coverage using Band 14 frequencies. The Offeror shall provide coverage maps (as outlined in Table 2 Coverage Maps Required for Coverage and Capacity) and network statistics (as described in Table 3 Network Statistics Required for Coverage and Capacity). The Offeror shall provide a proposed persistent coverage for Band 14 that addresses the desired coverage objectives as identified in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.1.1.4 Band 14 Population Coverage

The Offeror shall propose persistent population coverage using Band 14 frequencies. The Offeror shall overlay its proposed Band 14 area coverage maps (including the network analysis layers) with the 2010 U.S. Census 1 mile by 1 mile population count map (see Section J, Attachment J-1, Coverage and Capacity Definitions) and provide the proposed output population coverage statistics (by state/territory) using the Section J, Attachment J-17, Coverage and Capacity Template.

L.3.2.1.1.5 Band 14 Network Capacity

The Offeror shall provide Band 14 network projected demand and capacity statistics at the county level for FOC in Section J, Attachment J-17, Coverage and Capacity Template. Band 14 network capacity is the aggregate proposed design capacity and is computed by summing the average downlink throughput for each cell in a given county. County-based demand—as of 2015—is provided in Section J, Attachment J-1, Coverage and Capacity Definitions, as an input to the Offeror's projected demand at FOC. The Offeror shall describe its proposed process used to forecast Band 14 demand at FOC. The Offeror shall detail the available capacity for public safety and secondary users based on the proposed network. Excess network capacity is defined as capacity not used by Public Safety Entities (PSEs). The excess network capacity shall take into consideration the Offeror's projected highest amount of network usage by public safety during an hour per month as can be derived from the per county demand map in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.1.1.6 Planning Tool Analysis Layers

The Offeror shall provide the following LTE analysis layers for all Band 14 coverage maps noted in Table 2 Coverage Maps Required for Coverage and Capacity:

- Reference Signal Receive Power (RSRP)
- Best Server
- Downlink Signal-to-Interference-Plus-Noise Ratio (SINR)
- Uplink SINR
- Modulation and Coding Scheme (MCS)
- Downlink Average Data Rate
- Uplink Average Data Rate
- Composite Coverage Map

The Offeror shall provide network statistics for each of the LTE analysis layers (with the exception of the RSRP, Best Server, and Composite Coverage Map layers) using Section J, Attachment J-17, Coverage and Capacity Template.

L.3.2.1.2 RAN Strategy and Solutions

The Offeror's proposed RAN strategy and solution shall encompass architecture, design, and deployment strategies that effectively use resources, skill sets, an organizational structure, and tools. The Offeror's proposed approach shall demonstrate the capabilities described below and may include maps, tables showing relevant statistics, and brief descriptions of features and services.

The Offeror shall provide a list of air interface standards and/or non-standards to be implemented in the proposed network to enable communication between Enhanced Node Base stations (eNodeBs) and User Equipment (UE).

Heterogeneous networks (HetNets) may be an integral part of the NPSBN. The Offeror shall describe the types of heterogeneous RANs proposed by the Offeror that will be used by FirstNet UE to communicate with the Core network. The Offeror shall describe any HetNet implementation strategy and proposed deployment scenarios consistent with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline. The description shall include any applicable small cell solutions and associated LTE HetNet architecture, technologies, and equipment.

The Offeror shall describe the network sharing solution for Covered Leasing Agreement (CLA) users, ensuring sharing does not adversely affect public safety users and services. The Offeror shall detail the architecture and service differentiation methodologies for the proposed solution (e.g., Multi-Operator Core Network [MOCN]).

L.3.2.1.2.1 Features and Functionalities Impacting User Experience

The Offeror shall describe the features and services along with any relevant maps, tables, and applicable numeric descriptions. For each spectrum band and technology type the Offeror proposes, the Offeror shall describe the features and services available by proposed covered area type. The Offeror shall describe the user experience capabilities offered within the service area, (e.g., expected throughputs, Quality of Service [QoS], Access Class Barring, capacity thresholds on priority, location services, messaging, data caps, Voice over LTE [VoLTE]). The descriptions shall include supporting maps where applicable.

The Offeror's proposed solution shall describe any nationwide and international roaming capabilities offered to NPSBN users via network partners. The description may include the device frequency and features as well as the roaming network services provided to NPSBN users.

L.3.2.1.2.2 Network Planning and Design

The Offeror shall provide its proposed network planning and design information used for any submissions related to Band 14, including coverage and capacity submissions. This shall include the following documentation:

- **Link Budget** – Detailed link budget analysis sheet that aligns with the Section J, Attachment J-17, Coverage and Capacity Template, Link Budget Parameters tab. The link budget shall account for all assumptions, margins, and gains for both downlink and uplink. It shall be provided for hand-held and high-power UE, maximum allowable path loss, design thresholds, and cell radius for all morphologies (Dense Urban, Urban, Suburban, and Rural).
- **Link Curve** – Detailed link curve along with system simulation data showing the relationship between SINR, code rate, MCS, and throughput.

- **Planning Tool Settings** – Document settings used in the planning tool, including but not limited to Multiple Input, Multiple Output (MIMO) gains; clutter weights/losses; and environment configurations.
- **Geo-data description** – Detailed description of the geo-data used (e.g., clutter, terrain, clutter height, buildings), including but not limited to vintage, source, and resolution.
- **Propagation Models Description** – Detailed description of how the propagation models for planning were generated and if they are calibrated or un-calibrated. If calibrated models are utilized, describe how the models were calibrated.
- **Planning Project and All Supporting Folders** – Copy of the project file used in the Offeror's planning tool. All supporting files and folders needed to build a project shall be provided with the exception of the site summary data noted below. The project file shall include the analysis generated as well as traffic maps.
- **Site Summary** – Site summary that aligns with the Section J, Attachment J-17, Coverage and Capacity Template, Site Summary tab. A site table shall be provided for the FOC, including a field to identify the site information for each IOC. Site summary data is not required as part of the proposal submittal, but will be required 30 days after award as noted in Section F, Deliverables and Performance.

As part of the evaluation process, the Government reserves the right to request detailed site information (to include all site data for up to two counties per state or territory). If requested, these data are to be supplied using the "Site Summary" tab in Section J, Attachment J-17, Coverage and Capacity Template.

L.3.2.1.2.2.1 Network Design Statistics

The Offeror shall provide its proposed RAN solution for each of the 56 states and territories for each IOC and FOC milestone. The Offeror shall provide the following information in accordance with statistics required in the Coverage and Capacity Template (Section J, Attachment J-17).

- **Downlink SINR Distribution** – Average downlink SINR and distribution by proposed coverage area and population
- **Uplink SINR Distribution** – Average uplink SINR and distribution by proposed coverage area and population
- **MCS Distribution** – Downlink and uplink MCS distribution by proposed coverage area and population
- **Average Downlink Sector Throughput** – Average downlink sector throughput and throughput distribution by proposed coverage area and population
- **Average Uplink Sector Throughput** – Average uplink sector throughput and throughput distribution by proposed coverage area and population

L.3.2.1.2.2.2 RAN Technology Roadmap

The Offeror shall provide IOC/FOC milestone details of its proposed approach for the RAN technology roadmap that includes the applicable technology standards and releases, vendor equipment capabilities, features and services identified for inclusion into the NPSBN, and ways it specifically addresses the RAN public safety needs. The roadmap shall include the target availability date for the items described and shall identify the latest 3GPP release supported. The Offeror shall also provide the proposed RAN hardware, software/feature evolution roadmap, and insight into impacts to RAN nodes, antenna systems and interfaces.

L.3.2.1.2.2.3 NPSBN Vendor Infrastructure Equipment

The Offeror shall describe the proposed RAN vendor portfolio (outlining its proposed equipment suppliers and manufacturers), scope of equipment, and feature interoperability to be included with the NPSBN. Specifications are to be provided where applicable and shall include:

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

- A diagram and description of the LTE base station and sectors, including the antenna system and backhaul components. Identify areas of resource aggregation or redundancy and describe redundancy mechanisms available in the event a radio fails.
- A description of variant eNodeB platforms available in the current architecture, including specifications for each platform.
- Hardware or software techniques utilized to maximize coverage and capacity (e.g., MIMO, carrier aggregation).
- A dimensioning guide for all capacity-dependent hardware and software in the eNodeB. The guide shall describe the traffic load used in the dimensioning calculation as well as any assumptions made for redundancy.
- Solution details if antennae are shared with another frequency band.
- The maximum number of radio bearers supported by each variant eNodeB platform.
- Details for configurations in which a remote radio is involved (e.g., integrated antenna, separate antenna).
- A description of the RAN's congestion management capabilities that would be leveraged in heavy traffic situations.
- A description of which of the 16 3GPP-defined Random Access Resource configurations are supported by each eNodeB platform.
- A description of all RAN security features.

L.3.2.1.2.3 NPSBN Deployment

The Offeror shall describe its proposed nationwide approach to deploying the NPSBN, including any assumptions and considerations used to determine the proposed network offering and service area.

The Offeror shall describe the general design methodologies used to provide indoor and outdoor coverage. Specifically, the Offeror shall articulate with statistics the level of in-building coverage available at each IOC/FOC milestone for Band 14 and any non-Band 14 technologies using Section J, Attachment J-17, Coverage and Capacity Template. The metrics shall include the total available area for each of the 56 states and territories (in square miles), the area covered (in square miles), area covered (in square miles) with useable in-building signal levels, the total available population for each of the 56 states and territories, the population covered, and the population covered with useable in-building signal levels. In areas where in-building penetration from the macro network is inadequate, the Offeror shall describe techniques to enhance in-building coverage. Additionally, the Offeror shall identify which in-building solutions will be served with or without Band 14, including a list of locations for each in-building solution.

The Offeror shall describe the deployment strategy to serve different modes of transportation, such as tunnels, railways, ports and waterways, airports, and roads. The Offeror shall also provide the proposed design, methodologies, sources, and methods used to identify transportation infrastructure coverage requirements and the methodology to determine the appropriate level of indoor, outdoor, and underground service. In addition, the Offeror shall provide details on the approach to integration of in-building solutions with the NPSBN.

The Offeror shall demonstrate in its proposed solution how the capacity is planned beyond serving the public safety addressable market in a given state or territory. The Offeror shall present its strategy for maximizing excess capacity, while taking into consideration the highest amount of network usage by public safety during an hour per month derived from the per county demand map provided in Section J, Attachment J-1, Coverage and Capacity Definitions. The Offeror shall demonstrate the methodology or

the approach in determining the excess capacity that can be preempted during emergency situations. The Offeror shall describe its network hardening strategy (e.g., deployable strategy, selective site hardening, and self-organizing network [SON] for Public Safety Grade [PSG] services). The Offeror's strategy shall meet local building/construction codes and standards.

The Offeror shall concisely explain how it will ensure the RAN components, sites structures, radio equipment, and interconnection are designed and implemented to be resilient against failures that can disrupt services to first responders. The Offeror shall address redundancy strategies, including but not limited to the following:

- **Backup Power** – Provide, on a per state basis, the percentage and location of sites to be configured with backup power systems, the types of backup systems, and the average runtime between service for each of the 56 states and territories. Include detailed plans about portable generators.
- **Resilient Interconnection** – Provide, for each of the 56 states and territories, on a per state basis, the percentage of site infrastructures hardened against backhaul failure with multiple independent interconnections capable of individually handling expected traffic from the wireless facilities.
- **Weatherization** –Provide a strategy for how sites located in areas prone to adverse weather conditions, including but not limited to flooding, storm surges, tornados, earthquakes, hurricanes, ice storms, and wildfires, are addressed.

L.3.2.1.2.4 Network Operations and Performance

This section provides instructions to the Offeror on the information required regarding its proposed approach to network operations and performance. Should the Offeror elect to include a Mobile Virtual Network Operator (MVNO) or MVNO-like model in its solution, details shall be provided pertaining to that solution. These details are not required where an MVNO or MVNO-like model is not proposed.

L.3.2.1.2.4.1 Transition to Operations

The Offeror shall describe the proposed level of assistance provided to first responders to utilize the full capabilities of the NPSBN and any proposed MVNO. This assistance may include training on equipment, features, and services available for normal and emergency operations.

L.3.2.1.2.4.2 MVNO Key Performance Indicators and Acceptance Testing

The Offeror shall describe the end-to-end performance and operations of any proposed MVNO as well as the NPSBN. The description shall include the recent MVNO network performance KPIs and trends as well as the proposed acceptance test plan for the MVNO network performance, UE, and services. Network performance KPIs include but are not limited to:

- **Accessibility** – Address the probability of an end user being provided with an LTE radio bearer upon request. Include the percentage of successful attempts per overall number of attempts.
- **Retainability** – Address how often an end user abnormally loses an LTE radio bearer during the time that the radio bearer is being used. Include the percentage of abnormal session releases per session time units.
- **Integrity** – Address how the LTE network impacts the service quality provided to an end user or the delay experienced by an end user. Describe throughput (i.e., Internet Protocol [IP] data volume per time) and latency.

- **Availability** – Address when an LTE cell is available for service. Include the percentage of time that the cell is considered available.
- **Mobility** – Address how well the LTE mobility functions are working. Include the handover success rates.

L.3.2.1.2.4.3 Self-Organizing Network

The Offeror shall describe any SON features and services proposed for the Band 14 RAN in terms of self-configuration, self-optimization, and self-healing. The Offeror shall provide the strategy, integration timeline for SON capabilities, and architecture proposed for SON.

L.3.2.1.2.4.4 Deployable Units and Temporary Coverage

The Offeror shall describe the strategy for providing temporary incident-level coverage (Band 14 and non-Band 14) and addressing capacity issues using deployable units, satellite, direct mode, or a combination thereof. The proposed strategy shall describe how temporary coverage and capacity will be provided for areas that are not covered with persistent LTE services. The Offeror shall propose a single, nationwide strategy that describes regional variations. The Offeror shall also provide the following information in the strategy:

- Reference the five National Incident Management System (NIMS) types and planned events, specifically with respect to response time, coverage area, and required capacity.
- List permanent and temporary staging locations (e.g., in the event PSEs mobilize and pre-stage locations for hurricane or wildfire seasons) and proposed quantities of each type of deployable unit.
- Describe how deployable units will be integrated into the macro network and with other deployable units from a RAN perspective to avoid interference and enable handoff communications. Describe how deployable units will be integrated into the Core network and the types of available backhaul.
- Describe the operational aspects associated with each type of deployable, including activation methods, the typical time for deployment from request, operations and maintenance required, and associated costs.
- Describe the envisioned roles and responsibilities from PSEs, FirstNet, and the Offeror with respect to deployables and temporary coverage solutions. Propose a strategy on allowing PSEs to have ownership of deployable assets. Describe the service capabilities (e.g., voice, location, messaging and alerting, throughput, quality of service, priority and preemption) of each type of deployable unit and how the user experience may differ when using deployable units versus services available in areas of persistent coverage.

L.3.2.1.2.4.5 NPSBN RAN Enhancements

The Offeror shall describe the proposed strategy to support necessary network expansion. The strategy shall address coverage, quality, and capacity improvements to the NPSBN and include methodologies and thresholds used to trigger Offeror-defined actions. Improvements may be needed to address the following areas:

- **Coverage** – Extension of coverage to serve new areas (e.g., increase of service area footprint)
- **Capacity** – Additional capabilities to address network congestion (e.g., cell density)
- **Quality** – Improvement of existing capabilities to meet local performance objectives (e.g., strengthening indoor and outdoor coverage)

The Offeror shall provide a proposed framework to facilitate collaboration with local, state, tribal, and federal governments to improve the NPSBN service area and capabilities. The framework shall address shared or independent efforts to align the NPSBN demand and services. The Offeror shall detail the proposed expansion of in-building coverage via government-owned/supplied equipment and use of government property for placement of the Offeror's equipment.

The Offeror shall describe the proposed strategy, methodologies, and decision thresholds needed to improve:

- **Equipment/System Overlays** – Describe the process for repairing or replacing NPSBN equipment due to feature additions or changes in equipment vendors
- **Technology Migration** – Describe the process for system-wide migration (e.g., 4G to 5G).

L.3.2.1.2.5 Early Builder Integration

If the proposed solution includes early builder assets, the Offeror shall describe the proposed early builder assets and how they will be acquired, integrated, and assimilated. The Offeror shall describe the level of effort, strategy, associated risks, and timelines required to acquire, integrate, and assimilate the early builder assets in the respective geographic areas.

L.3.2.1.3 IOC Milestones for Coverage and Capacity

This section provides instructions as it relates to the target milestones set forth in Section J, Attachment J-8, IOC/FOC Target Timeline. Where Section L.3.2.1.1, Coverage and Capacity Maps and Statistics, requires coverage and capacity information at FOC on a per state/territory basis, this section requires details regarding coverage and capacity to be broken out for each of the IOC milestones. For additional instructions regarding the coverage maps and network statistics, see Sections L.3.2.1.1.1 through L.3.2.1.1.4, and apply them to the IOC milestones.

L.3.2.1.3.1 IOC Coverage Maps and Network Statistics

The Offeror shall provide the following LTE analysis layers for all Band 14 coverage maps as noted in Table 4 Coverage Maps Required for Coverage and Capacity.

- RSRP
- Best Server
- Downlink SINR
- Uplink SINR
- MCS
- Downlink Average Date Rate
- Uplink Average Data Rate
- Composite Coverage Map

The Offeror shall provide network statistics for each of the LTE analysis layers (with the exception of the the RSRP, Best Server, and Composite Coverage Map layers) using Section J, Attachment J-17, Coverage and Capacity Template.

Table 4 Coverage Maps Required for Coverage and Capacity

Level	Band	Phase	Maps Required	Format	Submittal Method
Nationwide	Non-Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5	Five (5) nationwide maps of each file format, depicting coverage by technology: LTE, 3G, 2G, and roaming layers.	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive
Nationwide	Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5	Five (5) nationwide maps of each file format, depicting the LTE analysis layers specified above	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive

* Note: If needed, the Offeror may provide multiple regional MapInfo & Esri (.shp) files that display coverage for smaller areas versus for the entire nation to fit within application and file size limitations. If regional maps are provided, they shall collectively represent nationwide coverage.

The Offeror shall provide the following network statistics in the Section J, Attachment J-17, Coverage and Capacity Template.

Table 5 Network Statistics Required for Coverage and Capacity

Coverage Type	Level	Phase
Non-Band 14 Area Covered **	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, and IOC-5
Non-Band 14 Population Covered **	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, and IOC-5
Band 14 Area Covered	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, and IOC-5
Band 14 Population Covered	State/Territory	IOC-1, IOC-2, IOC-3, IOC-4, and IOC-5
Band 14 Network Capacity	County	IOC-1, IOC-2, IOC-3, IOC-4, and IOC-5

** Note: Non-Band 14 coverage statistics shall be broken down by technology: LTE, 3G, 2G, and roaming.

L.3.2.1.3.2 Rural Coverage and Non-Rural Coverage

The Offeror shall indicate the proposed amount of persistent Band 14 rural and non-rural coverage for the nation as a whole and each of the 56 states and territories for the IOC/FOC milestones. The Offeror shall provide this information using the Section J, Attachment J-17, Coverage and Capacity Template. FirstNet-defined rural maps are provided in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.1.3.3 Network Deployment Timing

Using the Section J, Attachment J-17, Coverage and Capacity Template, Sites by IOC_FOC tab, the Offeror shall indicate how quickly the IOC/FOC milestones for Band 14 coverage will be met based on the proposed solution.

The Offeror shall indicate any risks in meeting the proposed deployment schedule.

Where non-Band 14 coverage is proposed, the Offeror shall describe timing for any partner, MVNO, or roaming networks that may be used.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

L.3.2.2 Products and Architecture

Offeror shall ensure that its solution aligns with industry standards as described in Section J, Attachment J-4, System and Standards Views.

L.3.2.2.1 Services

The Offeror shall describe its proposed solution for the following NPSBN services:

- Basic Network Services
- Quality of Service, Priority, and Preemption (QPP)
- Identity, Credential, and Access Management (ICAM)
- Mission-Critical Services

The Offeror shall provide, at a minimum, the following information for each service:

- Service architecture and design documentation
  - 3GPP standards implemented, including version numbers
  - External interfaces described in Section J, Attachment J-4, System and Standard Views
- Roadmap of service features and functionalities according to IOC/FOC milestones
- Design criteria and objectives for services of the NPSBN at the national, state, county, city, and rural levels
- Description of how the metrics outlined in the Offeror's proposed QASP will be used to monitor and manage the NPSBN service

L.3.2.2.1.1 Basic Network Services

The Offeror shall propose a strategy to provide basic network services to public safety users. If the Offeror includes existing commercial services in its solution, then the Offeror shall demonstrate evidence in achieving quality metrics in current deployments and how it will sustain performance improvements for the proposed basic network services solution.

The Offeror's solution, whether it is based on existing commercial services or not, shall address the following basic network services:

- **Messaging** – Describe how the solution supports text messaging, Multimedia Messaging Service (MMS), instant messaging, email, voice mail, chat, and Rich Communications Services (RCS)
- **Streaming Video/Audio Services** – Describe how video services will be incorporated and made available to users and applications
- **Voice telephony (VoLTE, VoIP, circuit switched, etc.)** – Describe how the solution supports voice communications throughout the coverage area in cellular and Wi-Fi and by interworking with IP private branch exchange (PBX)/Public Switched Telephone Networks (PSTN)
- **Machine-to-Machine Communications** – Describe how the solution supports device-to-device communications, machine-to-machine communications, and data exchange within the NPSBN as well as to and from external networks
- **IP Multimedia Subsystems Services** – Describe the architectural framework to deliver multimedia services, focusing on interoperability with another carrier's IP Multimedia Subsystem and third-party IP Multimedia Subsystem application providers
- **Broadcast and Multicast Services** – Describe the proposed broadcast and multicast services for bandwidth-intensive communications

- **Presence Services** – Describe proposed presence and discovery services
- **Location Services** – Describe proposed location-based services with accuracy for x and y coordinates
- **Device Management** – Describe proposed device configurations, accounting and logging, authentication, encryption, key management, lockdown, and status tracking for public safety users
- **Device Authentication** – Provide details on proposed mutual device-network authentication, encryption, and integrity protection for public safety users
- **Lawful Intercept** – Describe how the solution enables the Communications Assistance for Law Enforcement Act (CALEA) to intercept signaling and bearer information for specific users
- **Next Generation 9-1-1 (NG911) Services** – Describe how the solution supports interconnecting and sending information to a Public Safety Answering Point (PSAP)
- **Wireless Emergency Alerts (WEA)** – Provide details on how the solution supports WEA

L.3.2.2.1.2 Quality of Service, Priority, and Preemption

The Offeror shall provide a detailed description of the proposed strategy and design of its QPP solution for the NPSBN, including systems, interfaces, and settings. The solution shall ensure public safety users can access network services during emergencies in spite of network congestion. The Offeror shall describe the following QPP services:

- **QPP States** – Describe how the solution supports moving a cell or cells within the network between distinct operational states. Operational states include static state (i.e., the network relies on its configuration to ensure QPP, dynamic state (i.e., the network takes dynamic response data from public safety users to dynamically control QPP), and controlled state (i.e., a local agency is able to influence the dynamic state through local control).
- **CLA User States** – Describe how the solution supports control of CLA users on the NPSBN. CLA user states include free range (i.e., CLA users have full access to any unused network resource), restricted (i.e., CLA users are limited to a percentage of the network resource), and preempted (i.e., CLA users are removed from the NPSBN for a period of time in a defined geographic area).
- **Emergency User States** – Describe how the solution supports handling immediate peril services and responder emergency services for public safety users.
- **QPP Profiles and Static User Data** – Describe how the solution implements default and emergency QPP profiles for different users with different roles. Define the primary user type and default user roles.
- **Dynamic Data** – Describe how the solution supports dynamically changing data (e.g., user location, user operational status, incident role, incident identifier, incident location, incident severity). These data may be updated via an Application Programming Interface (API) or another method and will be used by the NPSBN to affect dynamic changes to QPP.
- **Application Profiles** – Describe how the solution creates application profiles with static and dynamic application QPP for each application. Application profiles shall include the application type, usage scenario, priority, QoS, preemption, frequency of use, and expected bandwidth.
- **Operational Profiles** – Describe how the solution groups application profiles into operational profiles that can be tailored for each agency.
- **Dynamic QPP Management** – Describe the overall service delivery, management, reporting, and technical approach for addressing FirstNet's QPP objectives.

- **Dynamic Controller** – Describe the solution that interfaces with the various network systems and Local Control to obtain user data (static and dynamic), network utilization, and triggers, as well as drive changes in QPP properties in real time.
- **Priority During Roaming** – Describe how QPP is managed, deployed, and operated while a first responder (priority user) is roaming on a commercial network.

L.3.2.2.1.3 Identity, Credential, and Access Management

PSEs are responsible for managing identity and credentials for first responders. The Offeror shall propose a federated and interoperable ICAM solution that allows public safety agencies to control identity and credentialing of first responders. The Offeror shall address the following areas:

- Describe how the solution improves security and data access for NPSBN users. Describe how the solution allows users of one agency to access data and services provided by a remote agency. Include details of the federated identity interfaces the solution supports and any impacts on an agency's infrastructure, processes, procedures, and applications.
- Describe how public safety agencies will be encouraged to participate in the ICAM solution, including timelines for onboarding and certification. Provide details on how the solution ensures agencies comply with and continue to follow ICAM requirements over time.
- Describe how the solution supports agencies that do not wish to host their own ICAM software and solution. Explain how the solution provides agencies a simple alternative that allows those agencies to fully participate in a federated ICAM solution and share and retrieve information with other public safety users/agencies.
- Describe how the solution supports managing credentials and ensures that credentials are secure and align with the Levels of Assurance (LOAs) as specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2 and referenced in Section J, Attachment J-4, System and Standards Views. Describe how the solution supports mobile device Single Sign-On (SSO) for both native and Web-based mobile applications. Describe how a user authenticates once and subsequently gains access to the applications using the previously used authentication credential/token. Describe how access to applications and/or services may require step-up authentication when the user provides a credential format/method that does not meet the credential strength requirements of that application/service. Describe how the mobile SSO solution can support different authentication methods and how those align with the defined LOA.
- Describe how the solution supports dynamic attribute-based access control (ABAC) and how applications protected by the solution authorize users before granting access. Provide information on the types of attributes that the solution supports. Include details on how the solution enables local agencies to manage user attributes and access policies.
- Describe how the Offeror proposes to support and evolve the ICAM governance processes and how the Offeror will support agencies adopting ICAM solutions. Provide relevant experiences and characteristics of the Offeror that demonstrate the Offeror's abilities to provide ICAM governance.
- Describe how the proposed solution supports multiple users sharing a device. Provide details on how authentication, authorization, and profiles are managed and supported on shared devices and include details on how each user's data is secured.

L.3.2.2.1.4 Mission-Critical Services

The 3GPP standards body is finalizing several mission-critical services required in the NPSBN to provide public safety users with emergency communication services. The Offeror shall describe its proposed roadmap and product development timing for mission-critical services in accordance with the IOC/FOC milestones outlined in Section J, Attachment J-8, IOC/FOC Target Timeline. Mission-critical services include but are not limited to:

- Enhanced LTE PSG Voice Telephony
- Mission Critical Push-to-Talk
- Broadcast Services for WEA
- Proximity Services (ProSe)
- Mission-Critical Data
- Mission-Critical Machine-to-Machine
- Mission-Critical Location Services (i.e., enhanced accuracy for x, y, and z direction and indoor locations)

L.3.2.2.2 Applications

The Offeror shall describe in detail its strategy and design for its proposed solution for applications, including the following key components:

- The software development methodology and rollout strategy
- The strategy to enhance and update software
- The strategy for soliciting and incorporating public safety input
- The applications release timelines as they relate to Section J, Attachment J-8, IOC/FOC Target Timeline
- Alignment with industry standards described in Section J, Attachment J-4, System and Standards Views
- Alignment with the application security standards described in Section J, Attachment J-10, Cybersecurity

The Offeror shall provide details on how the proposed solution supports performance, availability, reliability, scalability, resilience, manageability, security, and interoperability.

L.3.2.2.2.1 Applications Ecosystem

This section provides instructions related to the applications ecosystem in accordance with SOO Objective #5 in Section C, SOO.

L.3.2.2.2.1.1 Service Delivery Platform

The Offeror shall describe the proposed strategy regarding the following:

- The Service Delivery Platform (SDP) and how it is integrated with public safety APIs, the application development platform, and the network services layer.
- The network services described in Section L.3.2.2.1.1, Basic Network Services, which will be made available to the SDP. Include a proposed schedule of when those services will be made available and how those services will be made available to public safety applications and applications developers.

- The network services capabilities that need to be exposed using a common set of industry standards based on Section J, Attachment J-4, System and Standards Views.
- How the Offeror will develop services and applications policies for various scenarios, such as authorization, congestion management, privacy, API threats, and security. Explain how these policies will be monitored and analyzed.
- Details on any transformation, optimization, tuning, configuration updates, or enhancements that can be completed as a result of network and applications monitoring.
- How the SDP middleware and its application layer QPP policy are integrated with the LTE network layer infrastructure, including policy management.
- Service and application orchestration capabilities that the solution provides and/or capabilities that allow applications to orchestrate and call different services.
- Details on how services and associated applications that consume APIs can be orchestrated for both real-time and non-real-time public safety incidents.

L.3.2.2.2.1.2 Application Development Platform

The Offeror shall describe the proposed strategy regarding the following:

- How the solution supports and allows rapid third-party mobile application development.
- How the solution entices application developers to create applications for the FirstNet applications store.
- Development tools the solution provides and how the tools enhance developer productivity.
- How the solution exposes third-party developers to application development information, tools, Software Development Kits (SDKs), and other development capabilities.
- How the solution enables community support and collaboration tools that the solution provides, including chat, discussion fora, and message boards.
- Mobile application development frameworks the solution supports. Include details of how the framework supports application development and improves developer productivity.
- SDKs specific to developing public safety applications. Include SDK/API documentation. Provide details on APIs that will be exposed to applications. Include details on the network services APIs and additional services APIs, such as map tiles, analytic tools, or other services that the solution will provide.
- Test tools for developers to ensure that applications are free of defects and follow security and mobile application best practices. Note which tools test and/or analyze runtime code or static code. Explain how the tools support application testing throughout the development life-cycle, including before launch and after release.
- How the solution ensures that developers have a high level of confidence that the application will be certified and approved for publication in the FirstNet applications store. Include details on how developers perform application updates and versioning of their applications.

L.3.2.2.2.1.3 Hosting and Cloud Services

The Offeror shall describe in detail how the proposed solution supports cloud-hosted services and applications, providing rationale for why this is beneficial to FirstNet and PSEs. Specifically, the Offeror shall describe:

- How the solution supports hosting applications. Include descriptions of the tools and APIs the solution offers to application developers, Public Safety Enterprise Networks (PSENs), and PSEN

users that are hosting applications or services in the cloud. Include details of the benefits that users receive by hosting applications in the cloud solution.

- How it will provide different cloud services capabilities as they relate to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Describe how the solution will comply with FirstNet governance on security and standards.
- How the solution supports and provides data analytics and tools to public safety applications. Explain why data analytics are beneficial to FirstNet, PSEs, application developers, and public safety applications.

L.3.2.2.2.1.4 FirstNet Applications Store

The Offeror shall describe its proposed solution pertaining to the following:

- How the solution incorporates new applications into the FirstNet applications store, including the technical details, process, and governance required. Include details on the roles for public safety agencies, FirstNet, application developers, and the Contractor.
- How the solution handles payments and billing for applications and related services. Include details of the payment mechanisms and various pricing models (e.g., monthly recurring charge, one time) the solution supports. Describe how developers can choose the model that best fits their application.
- How the solution supports application change management, including the technical details, process, and governance required. Include details on the roles for public safety agencies, FirstNet, application developers, and the Contractor.
- How the Offeror will support or perform application updates and versioning to software that is provided to agencies and end users through the FirstNet applications store. Describe how the solution ensures that end users are informed of updates and critical patches. For applications provided directly by the Offeror, describe how the solution ensures users are properly trained on the updated software.
- The application life-cycle process, including details for each phase—from creation of the application through its retirement.
- How application customer support is provided to local, tribal, state, regional, and federal users and agencies.
- Additional FirstNet applications store capabilities that allow users to learn about applications capabilities and discover new applications. Include details on how these capabilities align with existing methods and tools that users may be using today.

L.3.2.2.2.1.5 Application Life-Cycle Management

The Offeror shall describe its proposed strategy pertaining to the following:

- The software development methodology that the Offeror and its subcontractors and/or teaming partners follow.
    - Include how feedback from FirstNet and NPSBN stakeholders will be incorporated into future applications ecosystem software releases.
    - Provide the process by which requirements for FirstNet public safety applications are driven through the development and deployment strategy.
- The schedule for each of the applications ecosystem deliverables identified in Section J, Attachment J-8, IOC/FOC Target Timeline. Include each of the capabilities in detail from sections L.3.2.2.2.1.1 through L.3.2.2.2.1.4, including initial release and update strategies.

- New processes for and enhancements to the applications ecosystem to ensure alignment with industry standards, particularly those outlined in Section J, Attachment J-4, System and Standards Views.
- The software update and sustainment strategy, including how to ensure the software continues to evolve and how to address defects. Provide details on how the application environment is agnostic to different mobile platforms, device capabilities, and network capabilities.
- How the application environment is optimized.

L.3.2.2.2.1.6 Developer and Application Certification

The Offeror shall describe its proposed strategy pertaining to the following:

- The application certification process, including details on the roles and responsibilities for FirstNet, the Contractor, public safety agencies, public safety users, and application developers. Provide details on the technical details, process, and governance required.
- The certification criteria recommended to ensure applications available in the FirstNet applications store are PSG in terms of security, identity management, robustness to malware threats, and resilient performance.
- The different certification levels that the solution supports. Include details on why different certification levels should be used and what the benefits are to FirstNet, public safety users, and application developers.
- The certification timeline for applications, including what circumstances may impact the length of time to certify applications.
- The types of testing required for an application to be certified. Provide details on how the solution tests an application's functionality, scalability, resilience, security, battery drain, and freedom from malware (intentional or unintentional).
- How the solution tests that the application runs correctly on different devices, operating systems, and software versions.
- Details on how the proposed solution will ensure that users maintain the expected level of service of the device and applications when they are on a local network with no backhaul connectivity or are off the network completely.

L.3.2.2.2.1.7 Application Security

The Offeror shall describe its proposed strategy pertaining to the following:

- How the solution provides application security and ensures that applications and the data used are secure for public safety users.
- How the solution protects data; prevents unauthorized access; and preserves privacy, data integrity, and data availability.
- How the solution will comply with the applicable security guidelines.
- How the solution ensures that the public safety user, agency, and application data are secure at rest, in transit, in use, and on the device.
- How the security posture of local agency applications and services can be viewed and how vulnerabilities can be identified.

L.3.2.2.2.2 Offeror-Provided Applications

In addition to an applications ecosystem, the Offeror is asked to explain its support for specific applications, including Local Control and a Public Safety Entity Home Page.

L.3.2.2.2.2.1 Local Control Application

The Offeror shall describe its proposed approach to providing a PSE user interface to each of the network services and Core network services. The Offeror shall describe how this interface enables a PSE to control its administrative and operational environments, including network services, operational support systems (OSSs), and business support systems (BSSs). The Offeror shall describe how the proposed approach addresses the following scenarios:

- An agency has one or more user roles
- An agency has one or more users
- A user has one or more user roles
- A user has zero or more devices
- A user has exactly one profile
- UE may be shared among users, but only one user at a time
- A device has one or more Universal Integrated Circuit Cards (UICCs)
- A UICC has one or more billing services assigned to be usable
- A QPP region has one or more PSEs operating in it
- An agency can operate in zero or more QPP regions

The Offeror shall also describe its support for:

- Event logging and auditing functions
- Onboarding and configuring for the specific needs of an agency
- Accommodation of local input into such topics as cell site locations, network topology, and use of local IP network resources

The Offeror shall describe its proposed strategy pertaining to how it will support the basic local control features listed below:

- Ability to add and remove a device to/from an account
- Ability to add and remove users to/from an account
- Ability to create, modify, and delete user groups and profiles
- Ability to assign users and user groups to user profiles
- Ability to assign applications to user profiles
- Ability to assign devices to users and user groups
- Ability to invoke QPP profiles during a simulated incident
- Ability to blacklist and whitelist applications

The Offeror shall describe how its proposed solution will address the following areas:

- Managing agency-specific policies for users, devices, services, and applications
- Encouraging agency acceptance of applications updates
- Providing local control over which applications may be downloaded and installed on a device
- Planning for “planned events”
- Handling unplanned outages
- Communicating with agencies regarding planned outages and system status
- Eliminating or mitigating outages during planned maintenance
- Tracking outages through resolution and root cause analysis and reporting

- Accepting and processing agency input regarding the planning, design, and construction of the NPSBN within the agency's service area
- Accepting and processing agency input regarding the device ecosystem
- Onboarding and supporting new agencies to the NPSBN and enabling interoperability at all service levels supported

The Offeror shall describe its proposed strategy pertaining to how it will support each of the ongoing network maintenance and expansion processes listed below:

- Describe how a local agency is made aware of service impairment.
- Explain how the Offeror proposes to provides a local agency with near real-time support to allocate network resources during an incident.
- Provide help desk support.
- Provide for a real-time local view of network status, performance, services, and any related trouble ticketing.
- Provide the ability for local agencies to request support and report service issues and impairments.
- Provide the ability to implement end-to-end network change management across each of the 56 states and territories.
- Provide the ability to troubleshoot individual subscriber calls within the Offeror's end-to-end network change management solution.
- Provide an interface into a back end for all operational logs and KPI data for continued service reporting and performance trending.
- Provide the ability for agencies to manage users and control user attributes and roles.
- Provide the ability for users to be recognized by other agencies.
- Provide mobile application management and describe how each agency may control user applications and services.
- Provide mobile device management. Describe how it allows agencies to manage agency and user devices and how it supports a Bring-Your-Own-Device (BYOD) ownership model.
- Describe the application that will be used to manage the priority and QoS of applications and users. Describe how the application allows for the control of user QoS for both voice and data communications.

L.3.2.2.2.2.2 Public Safety Entity Home Page

The Offeror shall describe its proposed strategy pertaining to the following:

- A customizable home page that provides users with relevant information about their agency and current events and incidents. Describe the home page's timelines for delivery and proposed functionality, including but not limited to the following:
    - Display current status of the wireless network
    - Display critical information of a general nature (e.g., news, weather, traffic)
    - Display critical and/or tactical information of agency-specific information (e.g., incident status, internal alerts, situational awareness data)
    - Support customizable services and data feeds that users can subscribe to, including NPSBN network and service status, agency information, alerts, and basic situational awareness of recent nationwide and local incidents

- How the solution will ensure that the PSE home page meets the needs of public safety agencies and users and how agency/user feedback will be incorporated into new releases of the PSE home page.
- Other forms of status alerting that can be used to notify an agency, such as email, Short Message Service (SMS), Rich Site Summary (RSS), FirstNet status page (as opposed to the PSE status page), and any other such "push" alerts.
- How affected agencies will receive ongoing, timely alerts when an outage impacts them without receiving unnecessary alerts until final resolution.
- How the PSE home page supports ABAC and the ability for local administrators to control what content is displayed and to whom. Explain how the home page can be used to provide access to non-local agency users during mutual aid scenarios.

L.3.2.2.3 Device Ecosystem

The Offeror shall describe the following capabilities associated with the device ecosystem.

L.3.2.2.3.1 Device Portfolio

The Offeror shall list all suppliers, model numbers, operating systems, software configurations, software clients, and embedded applications for the device portfolio. The Offeror shall identify advanced features and limitations across the portfolio for both single and multiple modem configurations. The Offeror shall use the Section J, Attachment J-11, Device Specifications Template, to describe the features and functions that each device in the proposed portfolio supports.

L.3.2.2.3.2 Band 14 Devices

The Offeror shall explain how its proposed device portfolio supports the following configurations for Band 14 devices:

- Smartphones, tablets, and modems that support Band 14 and combinations of other bands and the ability to maintain session continuity when switching from band to band
- In-vehicle routers that support multiple modems, including both Band 14 and combinations of other bands, and the ability to maintain session continuity when switching from band to band
- Vehicular Network Systems built into first responder vehicles that support in-coverage and out-of-coverage rapid response
- A wide variety of cost-effective device types and accessories to meet the needs of first responders
- Machine-to-machine or Internet of Things (IoT) configurations, including low-cost/low-power modems and configurations for video cameras, drone operation, and remote deployment(s)

In addition, the Offeror shall provide details on its proposed strategy pertaining to the following:

- Support for device management, application management, and a security container strategy as they apply to FirstNet standard devices and BYOD scenarios
- The ability to provision standard device and application management, configure standard device security, conduct over-the-air updates for firmware and applications, remove network access, and wipe devices
- For BYOD device support, the approach for onboarding of the device within the agency and systems, setting up the security configuration to support partitioning of FirstNet applications

and data, and removing network access and wiping the FirstNet data and application area of the device

L.3.2.2.3.3 Universal Integrated Circuit Card Management

The Offeror shall present its proposed UICC management program and describe the life-cycle support of profile(s) to operate across multiple networks. The Offeror shall highlight specific modifications that need to be made to current systems and processes to support the needs of public safety users, local control needs, and FirstNet requirements.

L.3.2.2.3.4 Device Management Client

The Offeror shall describe its proposed device management client solution, which shall fully interoperate with a standard Open Mobile Alliance–Device Management (OMA-DM) network solution. The Offeror shall provide documentation of IoT tests being validated with various device management vendors. The Offeror shall identify any extensions to the OMA-DM management and configuration objects needed for its devices and services.

The Offeror shall describe how the proposed device management client solution meets the following requirements with respect to FirstNet's device management:

- Support for remote management capabilities over the air, including software updates, discovery, device platform configuration, lock, unlock, wipe, security configurations, and other related abilities based on the OMA-DM protocol
- Enablement of local entities to install, update, and manage applications, including managing identification, notification, and removal

L.3.2.2.3.5 Device Approval Process

The Offeror shall supply the following certifications for current devices as part of its device approval process:

- Proof of Federal Communications Commission (FCC)-type certification
- PTCRB test reports after a device has been certified, including but not limited to:
  - TS 36.521 and TS 36.523
  - Uu Interface: 3GPP TS 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.314, 36.321, 36.322, 36.323, and 36.331
  - TS 36.306 UE Radio Access Capabilities
  - TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application
  - TS 31.103 Characteristics of the IP Multimedia Services Identity Module (ISIM) application
  - TS 31.111 USIM Application Tool Kit (USAT)
  - TS 37.571 Positioning
  - CTIA LTE IoT Test Plan
- Code Division Multiple Access (CDMA) certification forum test reports for any device that supports CDMA
- Battery certification reports resulting from the CTIA Battery Certification Program

Further information on the PTCRB test reports can be found in the permanent reference document NAPRD03, *Version Specific Technical Overview of PTCRB Mobile/User Equipment Type Certification*, available on the PTCRB website (www.ptcrb.com).

The Offeror shall identify all open issues and waiver requests. The Offeror shall identify the third-party test laboratory used and/or the mobile network operator laboratory that conducted testing, as well as a point of contact.

The Offeror shall propose an approach to carrier acceptance, referred to as the Device Independent Verification and Validation Test Plan, which can be used to certify public safety functionalities and features of mobile devices before the device is deployed on the NPSBN. The proposal shall provide an acceptance test plan for any of the Offeror's commercial band(s) if applicable to the Offeror's proposed solution.

The Offeror shall provide a roadmap of type certifications and respective standards for future devices.

L.3.2.2.4 Architecture and Infrastructure

The Offeror shall describe a proposed Core network solution, including the Evolved Packet Core (EPC), services, application platforms, and OSS/BSS, that is dedicated for public safety users. The solution shall be capable of integrating with the Offeror's RANs (Band 14 and non-Band 14) as well as state-deployed RANs.

The Offeror shall describe its proposed architecture for the Core network. The Offeror shall demonstrate evidence in achieving quality metrics in current deployments and describe how it will sustain performance improvements for the Core network solution.

The Offeror's description of its proposed architecture shall include but not be limited to the list below, and where applicable, the description shall include operational processes, metrics, and thresholds:

- Architecture descriptions and diagrams, including physical, logical, and geographic architectures
- High-level design criteria, objectives, and components
- Software releases and 3GPP standards (and their respective versions) implemented
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/FOC milestones, including components, functionalities, and design criteria evolutions
- Design criteria and objectives utilized for each of the 56 states and territories to maximize system availability, resilience, and reliability
- Failure restoration
- Degradation restoration
- Upgrade(s)/update(s), including the 3GPP upgrade process, to ensure timely deployment of public safety services that are being standardized in the future
- Deployment risk mitigation
- Capacity and traffic growth performance
- Traffic growth and capacity exhaust
- Roaming performance between Band 14 and any other networks
- Core network restoration during disasters and major incidents

L.3.2.2.4.1 Nationwide Core Network Architecture and State Integration

The Offeror shall provide its proposed nationwide Core network architecture and State integration plans.

L.3.2.2.4.1.1 Logical Architecture

The Offeror shall provide system views for all user and control planes for the following platforms, systems, and components:

- All network and service platforms, including SDP, IP Multimedia Subsystem, and EPC systems; transmission systems; location systems; presence systems; and security systems
- All BSSs, including billing, provisioning, asset management, CRM, customer portals, and financial systems
- All OSSs, including network management systems, element management systems, trouble ticketing systems, change management systems, and planned work/workflow systems
- All end-to-end security systems, including firewalls, intrusion detection systems, security gateways, border controls, monitoring, resolution, and investigation systems

L.3.2.2.4.1.2 Covered Leasing Agreement User Integration

The Offeror shall describe its proposed solution to integrate CLA users, including:

- Overall CLA user integration methodology and design
- How the solution ensures there are no adverse impacts to public safety users under normal operating conditions or challenging conditions (natural or man-made)
- Proposed quality metrics applicable to CLA users
- Compliance with 3GPP standards

L.3.2.2.4.1.3 Mobile Virtual Network Operator Strategy

If the Offeror elects to include usage of an MVNO in its proposed solution, then the Offeror shall provide its strategy for the MVNO network, including:

- A schedule of MVNO service availability to public safety
- Proposed capabilities to be offered under the MVNO
- A migration plan from the MVNO network to the NPSBN
- The quality specification and user performance of services and functionalities of the MVNO network
- A methodology of interworking between the NPSBN and MVNO network, including key considerations, parameters, and quality metrics
- A roadmap of MVNO strategy milestones that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline

L.3.2.2.4.1.4 Key Core Network Locations

The Offeror shall describe its proposed solution, including the information below, for key Core network locations (e.g., datacenters; switching, routing, and transmission hubs).

- Layout and configuration of Core locations
- Core location infrastructure, including mechanicals; fire suppression; racks; cabinets; primary power; back-up power; and heating, ventilation, and air conditioning (HVAC)
- Core location TIA-942 classification
- Core location type (e.g., owned or leased space, leased rack)
- Physical security access and egress policies

- Entrance facility redundancy and spatial diversity (e.g., power, transmission)
- Geographic zoning classification

L.3.2.2.4.1.5 Network Specifications, Design Criteria, and Operational Metrics

The Offeror shall provide a proposed strategy regarding network specifications, design criteria, and operational metrics (to be provided in the Offeror's proposed QASP; see Section J, Attachment J-6, Quality Assurance Surveillance Plan) for the following:

- Application platforms and enabling systems, such as IP Multimedia Subsystem, EPC systems, transmission systems, and OSS and BSS interfaces
- Non-standard or specialized equipment
- External network interconnection points such as PSTN, PSENs, Internet Service Providers (ISPs), and WSPs
- NPSBN, OSS, and BSS quality
- RAN/Core integration including the operations and maintenance interfaces between RANs and the Core in support of the NPSBN Services Management Center (SMC) (as described in Section L.3.2.2.5.3, Services Management Center)

L.3.2.2.4.1.6 Session Continuity

The Offeror shall describe its proposed strategy pertaining to how it will provide session continuity between the NPSBN and other networks for voice, data, and streaming sessions as well as signaling sessions. The Offeror shall describe how its solution achieves service continuity for each IOC and FOC milestone.

L.3.2.2.4.1.7 Roaming Strategy

The Offeror shall describe its proposed roaming strategy, including its solution for roaming between the NPSBN and any partner networks as well as other wireless systems while maintaining session continuity and appropriate QPP parameters. The Offeror shall provide a roadmap of roaming strategy milestones that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.1.8 Roaming Partner Integration

The Offeror shall provide its proposed approach for integrating roaming partners. The solution shall address how session continuity and appropriate QPP parameters will be impacted as users roam between Band 14 and other non-Band 14 networks.

L.3.2.2.4.1.9 IP Strategy

The Offeror shall provide its proposed IP strategy as it relates to IPv4 and IPv6. The Offeror shall outline its solution to distribute, assign, maintain, and manage public and private IP addresses. The Offeror's strategy shall include a roadmap to IPv6 that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.1.10 Heterogeneous Network Integration

The Offeror shall describe its proposed solution to integrate multiple networks (i.e., MVNO, Core, roaming partners, state-deployed RANs), as applicable, to form a seamless NPSBN. The Offeror shall outline its solution to maintain and manage this HetNet as well as ongoing network additions, upgrades,

updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its HetNet integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2 Transmission Systems Strategy

The Offeror shall provide a proposed transmission systems strategy that describes how the Offeror will support RAN backhaul, backhaul aggregation, a nationwide backbone transmission system and associated transmission security, routing methodologies, and service prioritization, including end-to-end QoS and priority integrity across LTE and transport layers. All integrated networks—e.g., MVNO, Core, roaming partners, and state-deployed RANs, as applicable—shall form a seamless interoperable NPSBN. The Offeror shall outline its solution to maintain and manage these transmission systems, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its transmission systems strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.1 RAN Backhaul Architecture, Topology, and Synchronization

The Offeror shall provide its proposed RAN backhaul architecture, topology, and synchronization approach across integrated networks (i.e., MVNO [if applicable], Core, roaming partners, and state-deployed RANs) and describe how it enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage RAN backhaul architecture, topology, and synchronization systems and components, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its RAN backhaul architecture, topology, and synchronization strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.2 RAN Backhaul Aggregation Transport Network

The Offeror shall describe the proposed architecture and design of its RAN backhaul aggregation transport network. The Offeror shall describe how it operates across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs) and how it enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage the RAN backhaul system aggregation transport network system and components, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its RAN backhaul aggregation transport network that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.3 National Transmission Network

The Offeror shall describe its proposed strategy pertaining to its national transmission network, which shall operate across any integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how the national transmission network enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage the national transmission network, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its national transmission network strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.4 Transport Security

The Offeror shall describe its proposed strategy pertaining to its transport security approach across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage transport security systems and components, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its transport security strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.5 Routing and Diameter Routing Agent Strategy

The Offeror shall describe its proposed strategy pertaining to routing and Diameter Routing Agent (DRA) approach across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage routing systems and components including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments and removals. The Offeror shall provide a roadmap for its routing and DRA strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.6 Transport Service Prioritization

The Offeror shall describe its proposed strategy pertaining to its transport service prioritization approach across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage the transport service prioritization, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its transport service prioritization strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3 Interconnection and Interworking

The Offeror shall describe its proposed approach to interconnection and interworking, including how it supports state-deployed RAN backhaul aggregation integration, PSEN and PSAP integration, PSTN integration, and Public Land Mobile Network (PLMN) integration with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage these connected systems, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its interconnection and interworking strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.1 State-Deployed RAN Integration

The Offeror shall describe its proposed approach to integrating state-deployed RANs with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage connections with state-

deployed RANs, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its state-deployed RAN integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.2 PSEN and PSAP Integration

The Offeror shall describe its proposed approach to integrating PSENs and PSAPs with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage these PSEN and PSAP connections, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its PSEN and PSAP integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.3 PSTN, ISP, and Peering Integration

The Offeror shall describe its proposed approach to integrating PSTN, ISP, and peering networks with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage connections with PSTN, ISP, and peering networks, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its PSTN, ISP, and peering integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.4 PLMN and Roaming Partner Integration

The Offeror shall describe its proposed approach to integrating PLMN and roaming partners with the Core network across all integrated networks (i.e., MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how the approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage these connections, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its PLMN and roaming partner integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.5 Support for Land Mobile Radio Network Integration (if proposed)

If the Offeror's proposed solution includes future plans for Land Mobile Radio (LMR) integration, the Offeror shall describe its approach, if proposed, to integrating LMR networks to the Core network across all integrated networks (i.e., MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage these connections to the LMR network, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its support for LMR Network integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.4 Public Safety Grade

The Offeror shall describe its solution to achieve PSG services for network reliability, resiliency, redundancy, environmental factors, and operational management approach.

L.3.2.2.4.4.1 Network Reliability

The Offeror shall describe its proposed network design and how it will ensure network reliability. The Offeror shall provide a benchmark for network reliability against existing commercial wireless operators.

L.3.2.2.4.4.2 Network Resiliency

The Offeror shall demonstrate its ability to provide and maintain an acceptable level of service as defined in SOO Objective #7, User Service Availability, in the face of natural disasters, faults, and other challenges to normal operation. The Offeror shall outline the solution and its ability to maintain and improve network resiliency for the NPSBN.

L.3.2.2.4.4.3 Network Redundancy

The Offeror shall describe its proposed solution to increase service availability through local and geo-redundancy solutions. The description shall include proposed methods for all layers of the network and associated quality improvement metrics gained as a result of this solution, especially in highly vulnerable key network nodes supporting mission-critical infrastructure.

L.3.2.2.4.4.4 Environmental Factors

The Offeror shall describe actions being taken in the design and implementation of the NPSBN to mitigate environmental factors that could adversely affect the performance of the NPSBN. The Offeror shall describe its proposed solutions for different regions impacted based on specific environmental factors (e.g., earthquakes, tornados, hurricanes, floods, fire) that could adversely impact the performance of the NPBSN (e.g., loss of core switch, loss of multiple sites covering an area, loss of large capacity connectivity). The description shall address each of the 56 states and territories.

L.3.2.2.4.4.5 Operational Management Approach

The Offeror shall describe how its proposed operational management approach is proactive and results in a continual improvement of network performance, services, and support for public safety users. The Offeror shall outline how it will report and communicate the network status, network impairments, and resolution status at a detail meaningful to local, state, and federal users. The Offeror shall describe past experience in proactive maintenance and introduction of new features, functionality, and applications without impacting user services.

L.3.2.2.4.5 Network Implementation

In this section, the Offeror shall describe various elements of network implementation, including integration with any partners or MVNOs, naming and identifying network nodes, design assumptions, numbering plans, number portability, and project plans.

L.3.2.2.4.5.1 Integration with Partners

The Offeror shall describe its proposed approach for integrating the NPSBN with partners. The integration includes all involved networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs).

L.3.2.2.4.5.2 Network Naming and Identification

The Offeror shall provide its proposed design/plan for naming and identifying network nodes for the NPSBN. The Offeror shall describe how this approach facilitates seamless implementation and operation of the network. The Offeror shall provide an approach for identifying public safety devices, RAN equipment, Core network equipment, telephone numbers, tracking areas, proximity-based services, LTE/Wireless LAN (WLAN) interworking, Evolved Multimedia Broadcast Multicast Service (eMBMS) service, group multicast calls, and group broadcast calls. The Offeror shall describe its naming and identification approach for at least the following items:

- International Mobile Subscriber Identity (IMSI)
- PLMN Identifier
- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Tracking Area Identifier (TAI)
- Access Point Name (APN)
- Global Unique Temporary UE Identify (GUTI)
- Global Unique MME Identify (GUMMEI)
- Cell Radio Network Temporary Identifier (C-RNTI)
- Packet Data Network Identity (PDN ID)
- Evolved Packet System (EPS) Bearer Identifier
- E-UTRAN Radio Access Bearer (E-RAB) Identifier
- Linked EPS Bearer Identifier
- Tunnel End Point Identifier
- International Mobile Equipment Identity (IMEI)
- Access network discovery and selection function (ADNSF) Server Name
- Temporary Mobile Group Identity (TMGI)
- ProSe Application ID
- Fully Qualified Domain Names for Security Gateway and Operations, Administration and Management (OAM) Systems

L.3.2.2.4.5.3 Design Assumptions

The Offeror shall provide the assumptions employed when designing the NPSBN network in accordance with Section L.2.6, Assumptions, Conditions, and/or Exceptions. The assumptions shall clearly identify responsible owners. The Offeror shall clearly identify any impact to quality metrics defined in the Offeror's QASP in case assumptions differ from implementation. The Offeror shall provide a three (3) to five (5) year forecast of assumptions that are relevant to the NPSBN network design.

L.3.2.2.4.5.4 Numbering Plan

The Offeror shall provide its proposed numbering/addressing schema for public safety devices. The Offeror shall provide the Integrated Services for Digital Network (ISDN) numbering plan, which complies with U.S. regulations, to assign public safety devices. The Offeror shall provide a schema on how device numbering will be mapped to user identities to support ICAM. In addition, the Offeror shall provide a network address approach for packet data communication between public safety devices and mobiles devices on other networks. The Offeror shall describe how the numbering and addressing plan supports public safety devices roaming in other PLMNs. The Offeror shall address how its approach supports both IPv4 and IPv6.

L.3.2.2.4.5.5 Project Plan/Schedule

The Offeror shall provide a proposed project plan and schedule for the implementation of the NPSBN. This includes but is not limited to RAN, Core, network services, transport network, applications, OSS, and BSS. The Offeror shall identify any variances with Section J, Attachment J-8, IOC/FOC Target Timeline, and the reasons for those variances. The Offeror shall provide a roadmap for the launch of the NPSBN that aligns with the IOC/FOC milestones.

L.3.2.2.4.5.6 MVNO to NPSBN Core/RAN Migration

Should the Offeror elect to implement an MVNO or MVNO-like model, then the Offeror shall describe its proposed approach to migrating public safety users from the MVNO to the NPSBN. This approach may include a number of phases (some of which are identified in Section J, Attachment J-8, IOC/FOC Target Timeline) but shall at least include migration to the Core network, NPSBN applications ecosystem, NPSBN devices, NPSBN services, and the scheduled rollout of the NPSBN RAN network.

L.3.2.2.4.5.7 Mobile Number Portability

The Offeror shall describe its proposed approach to mobile number portability. The Offeror shall describe how it will change the IMSI or mobile service provider without changing the ISDN number allocated to a public safety device. The Offeror shall provide the time frame of the porting process in accordance with Section J, Attachment J-3, FCC TAB RMTR. Support for number portability where an MVNO model is proposed shall also be described.

L.3.2.2.5 Operations

This section addresses proposed network and service operations, business and operational support systems, SMC, and service availability.

L.3.2.2.5.1 Network and Service Operations

The Offeror shall provide a clear, concise description that demonstrates how its managed services will meet the stated service availability objectives, as identified in Section C, SOO, for the NPSBN, including all services and applications provided. The Offeror shall describe its proposed strategy pertaining to the following:

- How an integrated service support model that is aligned with the Information Technology Infrastructure Library (ITIL®) or commercial equivalent will be delivered. The model shall include configuration, change, incident, and release management processes.
- The support personnel and systems used in the operations and fault diagnosis of the NPSBN. This shall include descriptions of support personnel and escalation procedures used in the investigation and resolution of anomalies, degradations, and impairments. Describe the tools used to verify call flows and messages between Core and RAN subsystems and test equipment to further diagnose or provide detection of system anomalies or degradations.
- Its NIMS processes and how the they enable effective communications with the incident commander and emergency operations center (EOC) in times of localized, regional, or national emergencies or incidents. These shall be consistent with Federal Emergency Management Agency guidelines and best practices and include:
    - A description of specific support organizations that are stood up in times of localized, regional, or national incidents that shall interface, coordinate, and support on-site incident commanders and EOCs

  - Reporting and communication practices to relay status and performance levels for local, state, and federal users
  - Reporting and communication practices to relay impairments and resolution status levels for local, state, and federal users
- Release management processes to introduce features, functionality, and applications into the NPSBN without impacting user services.
- Business continuity management processes, including provisions for disaster recovery and major event support to local, state, and federal agencies.
- Ongoing service-level management processes that provide a continued baseline of system and per service performance, including proactive improvement plans for increased performance, service, and support of NPSBN users. Include descriptions and examples of how service levels (meaningful to local, state, tribal, and federal public safety users) are reported to FirstNet.
- Availability management processes, including ongoing analysis of availability failures, contingency planning, and other activities and processes to ensure service availability objectives are met.
- Change management processes to support life-cycle NPSBN production changes and upgrades including software, hardware, asset deployment, and new asset integration. These shall include descriptions of how proposed changes and upgrades are submitted for review, approved, scheduled, and communicated to local, state, tribal, and federal agencies.
- Capacity management processes to meet current and future NPSBN objectives. These shall include descriptions of how the Offeror manages NPSBN utilizations, including computing, storage, network, and application sizing to ensure ongoing service levels.
- The national and local support structure to provide on-site support for both reactive and proactive configuration, maintenance, and monitoring activities. This shall include network optimization activities and quality assurance activities for the NPSBN.
- Protocols and processes to address state and local support of natural disasters and major events requiring deployable assets. The description shall include quantities of deployable assets and the default distribution of assets to support rapid response; procedures to request assets (both proactively and reactively); and deployment, operations, and support during such events.

L.3.2.2.5.2 Business and Operational Support Systems

The Offeror shall provide a clear, concise description that demonstrates how its proposed BSS and OSS will meet the stated objectives, as identified in Section C, SOO. The Offeror shall describe the following:

- The systems and interfaces in the application service to BSS and OSS. Include details on how the applications ecosystem provisions, charges (e.g., one-time, monthly recurring cost), and reports based on usage.
- The flexibility of the billing systems to define new profiles based on the agency usage billing models, throttling profiles, access to services/profiles, account types, and local control.
- The user, device, service, and application provisioning and management system(s) that enable and disable capabilities and provide information to the BSS in support of user adoption.
- The process utilized to ensure all regions are in sync with the billing and operational support system(s), including deployable units. Include how these systems report hardware, software, subsystem dependencies, and configuration-level consistencies or discrepancies.
- The back-end systems and interfaces that support the storage of historical system operational logs, system KPIs, performance metrics, billing transactions, and all other key files or logs needed for historical trending, records retention, and other performance management needs.

- The OSS's real-time ability to provide event-based monitoring correlating the different NPSBN subcomponent or network element alarming, including radio frequency systems, microwave backhaul, satellite backhaul, fiber backhaul, networking components, regional and Core LTE components, and application servers.
- The OSS's ability to provide real-time, performance-based monitoring and reporting around user onboarding and provisioning, user service experience, and individual NPSBN component performance that can be meaningful and applicable to an agency, tribe, or region.
- The capabilities and features of an electronic delivery mechanism(s) and format(s) that FirstNet personnel may use to conduct real-time and historical monitoring and investigation of network and service health, as well as usage and performance trending and analysis.
- The CRM systems used to capture and report on a user's life-cycle on the NPSBN. Include descriptions of how the system captures billing history, customer care interaction, current and historical performance, and technical support tickets and statuses for an individual user and agency.
- The trouble ticketing system for users reporting a degraded user experience on the NPSBN. Include descriptions of the workflow in investigating and resolving user issues; communication of current status or resolutions; and system's ability to detect, correlate, and alert out larger issues based on incoming ticket volume.

The Offeror shall show how a state that assumes responsibility for deploying its own RAN can also use the BSS and OSS effectively.

L.3.2.2.5.3 Services Management Center

The Offeror shall provide a clear, concise description that demonstrates the proposed structure of its SMC. The Offeror shall describe the following:

- The SMC location(s) and structure(s) that support the various network and service support functions, including applications, billing and provisioning, content services, devices, network (Core, RAN, Wide Area Network [WAN]), security, surveillance, and service desk.
- Technical support staff and resources available among each network and service function and how service troubleshooting is orchestrated by the SMC for varying levels of service. Detail how the SMC is made aware of all on-call staff spanning local/on-site locations to Core/national locations.
- The process of how public safety users originate a request or service issue into the SMC and how staff correlate and assess if a larger issue affecting users exists.
- Network and element management systems that provide real-time monitoring and dashboards of the end-to-end network. Detail how individual alarms are rolled up and correlated to service-based events. Include how SMC staff members are effectively prepared to respond, resolve, or route events to the appropriate next tier of support.
- How incidents are effectively managed and communicated based on the severity and location. Describe how an incident life-cycle is managed and effectively handed off between SMC shifts.
- KPIs around messaging of service status as well as its effectiveness in the identification and resolution of service degradation issues.
- Training plan for all SMC staff.
- Continuity staffing plan for key SMC positions.

L.3.2.2.5.4 Service Availability

It is FirstNet's objective to acquire services of a network designed to operate during natural and man-made disasters with restoration of services to the NPSBN taking precedence over other services. Availability is to be measured based on user data sessions and calculated as a percentage of successful user data sessions relative to attempted user data sessions for the reporting area and time period.

The Offeror shall propose how data sessions (successful, unsuccessful, and attempted) will be measured and reported. The Offeror shall also propose definitions of geographic reporting to ensure users and their agencies receive reliable service. The Offeror shall include its overall network design and operations strategy for providing high availability with special attention to those areas identified in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.2.6 Security

The Offeror's proposed solution shall encompass the design, architecture, and operational and testing plans with respect to cybersecurity of the NPSBN.

L.3.2.2.6.1 Public Safety Security

The Offeror shall provide a clear, concise description regarding its proposed approach to protect the network from cyberattack while maintaining reliable access. This description shall include but is not limited to the following considerations:

- **Usability** – Provide details on how the proposed solution will establish protective mechanisms that function effectively without adversely affecting network access.
- **Mission Primacy** – Outline and document how the proposed security mechanisms ensure uninterrupted or minimal degradation to the public safety mission.
- **Operational Security** – Provide details on how public safety data are protected while in transit and at rest.
- **Responder Safety** – Provide details on how the proposed solution will ensure the ability to request emergency assistance from first responders in mission performance or under immediate peril.
- **Reliability/Resiliency** – Provide details on how the solution will ensure service availability of the NPSBN.
- **Data Protection** – Provide details on how the proposed solution will safeguard Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), and Payment Card Industry (PCI) data.
- **End-to-End Protection of Data** – Provide details regarding the end-to-end protection of data by using encryption or other related methods and technologies.
- **Privacy** – Provide details on how the proposed security mechanisms across the NPSBN will ensure protection of personal data traversing the NPSBN.
- **Authentication** – Provide details on proposed authentication methods and technologies to ensure consistent access. The solution shall include, at a minimum, a federated ICAM solution with associated multifactor authentication.
- **Multi-Layer Security** – Provide details on how the proposed solution will permit individual PSEs to layer local security requirements onto the NPBSN for maximum flexibility within their respective jurisdictions.

- **Federal Information Security Management Act (FISMA) Compliance** – Provide details on how the proposed solution will permit relevant entities to ensure compliance with applicable requirements under FISMA when using the NPSBN.

L.3.2.2.6.2 Architecture Security

The Offeror shall provide a clear, concise description regarding its proposed approach to secure and protect the architectural components of the NPSBN within the context of public safety and accepted industry best practices. The description shall include but is not limited to end-to-end security management and logging, private encryption key management infrastructure, security policies and practices, fraud prevention and revenue assurance, network address translation support, protection between users, signaling storms, rogue or spoofed devices, HetNet support, Domain Name System (DNS) security, messaging security, IP Multimedia Subsystem security, BSS, OSS, mobile Virtual Private Network (VPN) support, business continuity and disaster recovery, IP infrastructure network elements, security hardening, cybersecurity, governance, cyber supply chain, insider threat mitigation, cloud environments, virtualization, software-defined networking, and VoIP spam**.** In addition to these elements, the Offeror shall include the following:

- **Security Integration and Testing** – Provide, at a minimum, the methods and approach for onboarding software/hardware and applying updates with associated testing to ensure optimal functionality within the approved security architecture. This includes mitigation strategies for required updates that may potentially introduce operational impacts.
- **Architectural Considerations** – Describe how the solution meets the requirements specified in Section J, Attachment J-3, FCC TAB RMTR.
- **3GPP Standards** – Describe how the solution adheres to 3GPP standards for cellular communication for both voice and data.
- **GSM Association (GSMA) Specifications** – Describe how the solution meets applicable GSMA specifications as outlined in Section J, Attachment J-3, FCC TAB RMTR.
- **Transport** – Provide details regarding the protection of data while in transit through appropriate use of encryption, access control, and other accepted policies and technologies. This includes data traversing external interfaces.
- **Domains** – Provide details regarding effective end-to-end protection and security of the indicated domains, including but not limited to:
    - RANs within each state and territory (either FirstNet-deployed or state-deployed)
    - Backhaul network, including eNodeB to regional aggregation points
    - Aggregation network, including aggregation of traffic in a region
    - National transport networks, including network connections to regional and national Core sites
    - EPC
    - BSS
    - OSS
    - Applications ecosystem
    - IP Multimedia Sub-System
    - Value-added services
    - Messaging services
    - PSE network connectivity
    - NPSBN cloud environments

L.3.2.2.6.3 Device Security

The Offeror shall provide a clear, concise description regarding its proposed approach to protect various aspects of the device ecosystem. This includes but is not limited to securing the operating system architecture, authentication mechanisms used for users and applications, embedded applications, mobile device management (MDM) and mobile application management (MAM), PSE-managed whitelist/blacklist, digital signatures of applications, and device security, including for BYOD, applications, and wearables.

L.3.2.2.6.4 Applications Security

The Offeror shall provide a clear, concise description regarding its proposed approach to protect elements of the applications used within the NPSBN. This description shall include but is not limited to the applications ecosystem, APIs, application software development life-cycle, application security certification, application vulnerability management, application developer certification, user logging, end-to-end application, application-specific port monitoring and validation, application and device security, data loss prevention, and secure application coexistence.

L.3.2.2.6.5 Identity, Credential, and Access Management Security

The Offeror shall provide a clear, concise description regarding its proposed approach to effectively secure ICAM. The description shall include, at a minimum, the following key elements:

- ICAM with federated identity from PSE networks
- Identity Assurance:
    - User to Device – PSEs may share a device between several first responders, necessitating the agency to identify which user has the device
    - Device to Network – LTE authentication
    - Network to Application – Identity management
    - Network to PSE Network – Identity management
    - User to Application – Identity management
    - User to PSE Network – Identity management
- Authorization
- Credentialing

L.3.2.2.6.6 Cryptographic Employment

The Offeror shall provide a clear, concise description regarding its proposed approach to effectively mitigate attack vectors against the IP-based infrastructure by employing encryption.

L.3.2.2.6.7 Public Safety Enterprise Network Security

The Offeror shall provide a clear, concise description regarding its proposed approach to formulate and implement minimum security standards to enable Public Safety Enterprise Networks to connect to the NPSBN.

L.3.2.2.6.8 Cybersecurity Life-Cycle

The Offeror shall describe its proposed cybersecurity life-cycle, including, at a minimum, how the Offeror will identify vulnerabilities and threats, determine risks arising from threats and vulnerabilities, prioritize risks to determine which warrant associated controls to address threats or vulnerabilities,

specify and implement controls to address or mitigate those threats and vulnerabilities, assess the effectiveness of controls, and monitor the security of the system.

L.3.2.2.6.9 Cybersecurity Systems Engineering

The Offeror shall provide a clear, concise description regarding its proposed approach to effectively ensure sustained security of all NPSBN environments. At a minimum, the Offeror shall:

- Enumerate operational policies and procedures to ensure that the cybersecurity system engineering approach is followed at all levels.
- Include repeatable processes that are executed continuously during the development and evolution of the NPSBN.
- Ensure cybersecurity engineering is considered in all decisions, designs, and actions.
- Ensure the network is used only by authorized personnel.
- Ensure the network and its users are protected from others, including external adversaries and insider threats.
- Ensure the cybersecurity program is robust.
- Ensure the design of the network and its components are secure by facilitating a cybersecurity assessment and utilizing resilient design principles.
- Establish processes for application security policies and procedures, and distribution of applications to be used on the NPSBN.

L.3.2.2.6.10 Risk Management

The Offeror shall provide a clear, concise description regarding its proposed risk management methodology, which should be executed continuously during the system development life-cycle and throughout the life of the contract and the NPSBN. The methodology may be based on or enhanced by a number of existing models, such as the NIST Risk Management Framework or the ISO 27000 series. The methodology shall include, at a minimum, the following:

- Asset identification
- Risk impact analysis
- Threat assessment
- Risk mitigation
- Security control selection and deployment
- Risk mitigation operations and maintenance

L.3.2.2.6.11 Cybersecurity Incident Response

The Offeror shall provide the Government with a documented Cybersecurity Incident Response Plan that includes but is not limited to computer security monitoring to rapidly detect incidents, vulnerability detection and analysis, log collection and analysis, tracking and reporting of incidents, and restoration of information technology (IT) operations after an incident occurs. The plan shall include specific technical processes, techniques, checklists, and forms to be used by the incident response teams. The Contractor shall document methods to report and escalate incidents to FirstNet in a timely fashion.

The Offeror shall provide a clear, concise description regarding its proposed approach to cybersecurity incidents. At a minimum, the Offeror shall describe how it will:

- Coordinate the notification and distribution of a cybersecurity incident.

- Mitigate the risk of an incident by minimizing disruptions.
- Notify the Contracting Officer if it appears that the mitigation will have an associated cost.
- Assemble security staff to conduct a threat analysis and resolve the incident.
- Take reasonable steps to mitigate the effects and minimize any damage resulting from the incident.
- Monitor system logs for application to the incident.
- Categorize all cybersecurity incidents per policy and procedure and report them within specific time frames.
- Define and capture metrics that will be used for reporting capability.
- Provide a post-mortem for each incident associated with an actual cyberattack in a format agreed upon by FirstNet and the Contractor.
- Provide an after action report for any incident that occurs due to inadvertent actions by authorized operations and maintenance personnel in a format agreed upon by FirstNet and the Contractor.
- Record and log all cybersecurity incidents into an electronic format.
- Report all cybersecurity incidents based on incident severity, as directed in standard operating procedures that will be developed jointly between FirstNet and the Contractor.

L.3.2.2.6.12 Security Operations Center

The Offeror shall provide a clear, concise description regarding its proposed security operations center. This shall include technologies employed, reports provided, logging approach and related forensic analysis of those logs, and incident response capability, as well as mitigation processes and related escalation procedures and criteria. The Offeror shall describe how it will, at a minimum, do the following:

- Collect, maintain, and share information about threats to network infrastructure, devices, data, and applications.
- Provide 24/7/365 cybersecurity monitoring of network infrastructure, devices, data, and applications.
- Provide monitoring and analysis of user, system, and network access.
- Assess the integrity of the NPSBN and associated data.
- Establish a baseline for network activity and utilization.
- Recognize and analyze activity patterns that are indicative of an incident or intrusion.
- Analyze logs for abnormal patterns.
- Establish information sharing and collaboration that integrates and disseminates information among critical infrastructure partners.
- Process, generate, and post suspicious activity reports.
- Provide assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications.
- Provide recommendations to partners and FirstNet leadership.

L.3.2.2.6.13 Continuous Diagnostic Monitoring and Mitigation

The Offeror shall provide a clear, concise description regarding its proposed approach to support continuous diagnostic monitoring and mitigation. The approach shall include but is not limited to hardware and software asset management, vulnerability management, configuration settings management, continuous network and system monitoring, and mitigation strategies.

L.3.2.2.6.14 Cybersecurity Testing and Certification

The Offeror shall provide a clear, concise description about its proposed approach to cybersecurity testing and certification. The Offeror shall describe how it will:

- Establish processes to verify security approaches through a life-cycle of selection, procurement, integration, and operations support. The testing methods shall include assessment, testing, examination, and interviewing. All testing results shall be retained to provide baseline standards for ongoing testing to ensure optimal accuracy and reproducibility.
- Validate individual systems
- Test integrated configurations
- Test independent applications and services, including the following:
    - New applications at the national level
    - User-developed or state-developed applications
    - Upgrades to approved applications
    - Security patches to approved and fielded applications

L.3.2.2.6.15 Network and Configuration Management

The Offeror shall describe how it will conduct tracking, planning, development, and implementation of new computer network defense/cybersecurity capabilities into all NPSBN systems. The Offeror shall provide documented methods, techniques, and processes to ensure that the configuration of device level, network, applications, and related components are known and changes are captured prior to implementation.

The Offeror shall provide a clear, concise description of procedures to address the following areas:

- Network management
    - Configuration management
    - Configuration identification
    - Configuration control
    - Configuration status and accounting
    - Configuration verification and audit
- Vulnerability management
- Patch management
- Centralized security log management
- Security information and event management

L.3.2.2.6.16 Environmental and Physical Security

The Offeror shall provide a clear, concise description regarding its proposed approach to environmental and physical security. The Offeror shall address, at a minimum, the following elements: power failure, humidity detection, cabinet door alarms, uninterruptable power supply power failure, access control to and within a facility, monitoring and recording of activity within a facility to include egress/ingress, movement activity within a facility after hours or in restricted areas, HVAC failure or degradation, building door alarms, generator failure, low generator fuel, low battery, closed caption television (CCTV) video surveillance systems, fire/smoke detection sensors, and protection from natural disasters (e.g., lightning/surge protection, water leak detection).

L.3.2.2.6.17 Information Security and Data Sensitivity

The Offeror shall provide a clear, concise description about its proposed approach to information security and data sensitivity. The Offeror shall, at a minimum, describe how it will:

- Encrypt and/or handle all data in transit, stored, or accessed across NPSBN environments as restricted data.
- Limit the use, dissemination, and access of restricted data to specific agencies, individuals, and situations.
- Establish mandated sensitivity and protection levels to data repositories used by FirstNet users.
- Ensure data retention follows existing record retention policies as specified by the respective data or system owner. Upon expiration of the retention period, data shall be destroyed or otherwise disposed of per agency policy.
- Prevent the release of data housed in the NPSBN to any external parties without compliance with applicable law.

L.3.2.2.7 Test Strategy

FirstNet expects to use the FirstNet Test Lab (FNTL) to test, verify, and validate features unique to public safety, as well as other devices and/or applications that may be critical to public safety, prior to their deployment into the operational NPSBN. Features unique to public safety include but are not limited to QoS, priority, preemption, and Mission-Critical Push-to-Talk. In addition to verification and validation, the FNTL will be used as a demonstration platform for NPSBN capabilities, training, and—in some cases—isolated troubleshooting of field issues. The FNTL will also be available for troubleshooting of these features should this be helpful.

The Offeror shall describe its proposed approach for providing Contractor-furnished equipment for the FNTL that will be utilized during acceptance testing for each IOC as well as any other testing FirstNet deems necessary and/or appropriate. The Offeror shall complete Table 1, Contractor-Furnished Equipment, included in Section J, Attachment J-15, noting the equipment that will be required to execute testing of features unique to public safety. This equipment is to be supplied by the Contractor.

The Offeror shall complete the Test Strategy Template included in Section J, Attachment J-12, describing its proposed approach to verifying and validating the products, features, and functions that support the NPSBN. The Offeror shall note those functions that are to be tested prior to IOC and FOC acceptance, as well as where these tests are to take place using Section C, SOO; Section J, Attachment J-3, FCC TAB RMTR; and Section J, Attachment J-8, IOC/FOC Target Timeline as references. Some features may be tested in an operational, deployed network, while others may be tested in a lab environment.

L.3.3 Volume III – Pricing

There is no page limitation for this volume. The Excel spreadsheet shall be submitted to reflect the information as stated herein and as contained in the Pricing Template (Section J, Attachment J-13). Each text page shall use Times New Roman Font Size 12, single spaced, double-sided, 8.5” x 11” (no exceptions allowed).

Certified cost or pricing data are not required for this procurement. The Contractor agrees to hold the price in its proposal firm until award or as requested in any subsequent amendment.

The failure to submit any of the information requested in this RFP may lead to the rejection of your proposal without further consideration.

The Offeror shall provide a glossary of abbreviations and acronyms used with an explanation for each. Glossaries do not count against the page limitations for their respective volumes.

The pricing volume shall contain the following information and be broken down in the following sections.

L.3.3.1 General and Structural Requirements

The Offeror shall complete the Pricing Template utilizing the Microsoft Excel electronic file provided in Section J, Attachment J-13. The Offeror shall complete all cells shaded yellow. The Offeror shall not password protect the completed Pricing Template. The Pricing Template shall not contain circular references; hidden sheets, columns, rows, or cells; or links to other files.

The Offeror shall complete the Pricing Template in order to propose the payments associated with task orders described in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders.

The Offeror shall enter positive values of the payments to FirstNet as positive numbers and negative values of the payments to FirstNet as negative numbers (as detailed in Section L.3.3.2, Payments to the Contractor).

All costs or prices provided shall be rounded to the nearest dollar. All proposal amounts shall be in U.S. currency.

The Offeror shall complete the following worksheets:

- **Payments to Contractor Worksheet** – Offerors shall propose payments to the Contractor as instructed in Section L.3.3.2, Payments to the Contractor.
- **Payments to FirstNet Worksheet** – The Offeror shall propose payments to FirstNet as instructed in Section L.3.3.3, Payments to FirstNet.
- **Delayed Payments to FirstNet Worksheet** – Offerors shall propose delayed payments to FirstNet as instructed in Section L.3.3.4, Delayed Payments to FirstNet.
- **Gross FirstNet Value Worksheet** – Offerors shall propose the gross FirstNet value as instructed in Section L.3.3.5, Gross FirstNet Value.
- **State Cost Worksheet** – Offerors shall propose state- and territory-specific costs as instructed in Section L.3.3.6, State-Specific Costs.

The Offeror shall reference the following output and calculation sheets but shall not amend them:

- **FirstNet Minimum Payment Thresholds Worksheet** – This worksheet shows the FirstNet minimum payment thresholds as identified in Section L.3.3.7, FirstNet Minimum Payment Thresholds.
- **Net Present Value Worksheet** – This worksheet shows the net present value as identified in Section L.3.3.8, Net Present Value Assumption.
- **Compliance Checks Worksheet** – This worksheet shows compliance checks that shall be met by the Offeror's proposal.

The Offeror's gross FirstNet value and all state-specific costs may inform the National Telecommunications and Information Administration's potential grant program for any states and territories that assume responsibility for deploying, operating, and maintaining their own RAN as authorized in section 6302 of the Act.

L.3.3.2 Payments to the Contractor

In its pricing volume, the Offeror may assume payments up to the aggregate total of $6.5 billion of budget authority. These payments to the Contractor may be made upon successful achievement, approved by FirstNet, of each IOC and FOC, for the Day 1 task orders and each state and territory RAN.

The Offeror may propose the drawdown of payments, subject to the following parameters:

- Aggregate payments to the Contractor may not exceed $6.5 billion.
- All payments to the Contractor shall be drawn down in accordance with the Act but no later than the end of fiscal year 2027.
- Payments to the Contractor for the Day 1 task orders must not exceed the nationwide elements maximum of $1 billion. Aggregate payments to the Contractor for each IOC/ FOC milestone on a nationwide basis must not exceed $1.5 billion.
- Offeror should assume availability of all $6.5 billion for purposes of its submission and ultimate evaluation, although this amount may be reduced after contract award depending on the identity and number of states that assume responsibility for deploying their own RANs.
- Offeror is to provide estimated IOC/FOC completion dates consistent with the Pricing Template (Section J, Attachment J-13) as it correlates to the Offeror's proposed solution.

L.3.3.3 Payments to FirstNet

The Offeror shall propose payments to FirstNet that will be the aggregation of positive and/or negative values that it proposes for the deployment and operation of initial FirstNet-deployed RAN states. The Offeror shall propose the values of the payments to FirstNet for each of the 56 states and territories.

The total sum of these values will be the nationwide payments to FirstNet, which must be at or above the minimum payment thresholds as set out in Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet Operational Sustainability. Note that Offerors are permitted to propose a negative value for any state or territory. Additional details regarding these payments are available in Section B, Supplies or Services and Prices/Costs, Section B.2.2, State and Territory Task Order(s) – Initial FirstNet-Deployed RAN States, and Section B.2.3, State and Territory Task Order(s) – Delayed FirstNet-Deployed RANs.

Pursuant to Section M, Evaluation Factors for Award, Section M.4.5.1, Net Present Value of Payments to FirstNet, the Net Present Value of the payments to FirstNet will serve as the basis for evaluating the pricing of the Offeror's proposal.

The payments shall adhere to the following parameters:

- For proposal preparation purposes, Offerors are to assume that year 1 of the pricing template commences on the estimated IDIQ award date (as defined in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders).
- Offerors shall provide payments to FirstNet over an assumed 25-year life of the contract consistent with the proposed levels in the Pricing Template (Section J, Attachment J-13).

- Offerors should note that the estimated IDIQ award date and task order date in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders, are included for RFP planning and proposal preparation purposes only.
- All sums in the Pricing Template (Section J, Attachment J-13) shall be rounded to the nearest dollar.
- [deleted in its entirety]
- The first payment to FirstNet will be due two weeks after the state and territory task order award date (Section G, Contract Administration Data, Section G.6.2, Payments to FirstNet), regardless of date of task order award. The first payment amount will be the proposed year 1 payment in the Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13).
- Billing in each subsequent Government fiscal year will occur two weeks prior to the start of the Government fiscal year.
- [deleted in its entirety]
- The Offeror's proposed payments are severable at the state level.

If, after receipt of proposals, the Government determines there is insufficient information available to determine price reasonableness and/or to ensure a meaningful evaluation in accordance with Section M, Evaluation Factors for Award, and none of the exceptions in FAR Part 15.403-1 apply, the Offeror may be required to submit additional cost or pricing data. Information shall be provided in accordance with FAR Part 15.403-5.

L.3.3.4 Delayed Payments to FirstNet

States and territories may initially opt to undertake responsibility for the deployment and operation of their RAN, but fail to meet statutorily required approval criteria, resulting in FirstNet deciding to take responsibility for the RAN. To accommodate these scenarios, the Government intends to include options for the Contractor to provide its proposed technical solution for those states and territories. The Government may exercise the task order(s) within 900 calendar days of the state plan delivery by FirstNet to the Governor of that respective state or territory, and this will be addressed through task orders described in Section B, Supplies or Services and Prices/Costs.

The Offeror shall propose values (positive and/or negative) of the payments to FirstNet for each of the 56 states and territories based on potential delayed FirstNet-deployed RANs.

The payments shall adhere to the following parameters:

- For proposal preparation purposes, Offerors are to assume that year 1 of the pricing template commences on the estimated IDIQ award date (as defined in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders).
- Offerors shall provide payments to FirstNet over an assumed 25-year life of the contract consistent with the proposed amounts in the Pricing Template (Section J, Attachment J-13).
- All sums in the Pricing Template (Section J, Attachment J-13) shall be rounded to the nearest dollar.
- First payment to FirstNet will be due two weeks after the state and territory task order award date (Section G.6.3, Delayed Payments to FirstNet). First payment amount will be the proposed year 1 payment in the Delayed Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13).

- Each subsequent payment will be due two weeks prior to the start of the subsequent Government fiscal year (Section G.6.3, Delayed Payments to FirstNet), and will continue until the end of the 25-year period of performance of the IDIQ contract.
- The last payment amount may be adjusted pro rata to align the Offeror's proposal with the respective Government fiscal year and the end of 25-year period of performance of the IDIQ contract.
- Due to the timing of the award of Delayed Payments to FirstNet, all Delayed Payments to FirstNet that were proposed by the offeror and are beyond the 25-year period of performance of the IDIQ contract will not be required.
- The Offeror's proposed payments are severable at the state level.

See Figure 1 Notional Contracting Process – Initial Years of IDIQ Contract, and Figure 2 Notional Contracting Process – Final Years of IDIQ Contract for further clarification of the contracting process.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

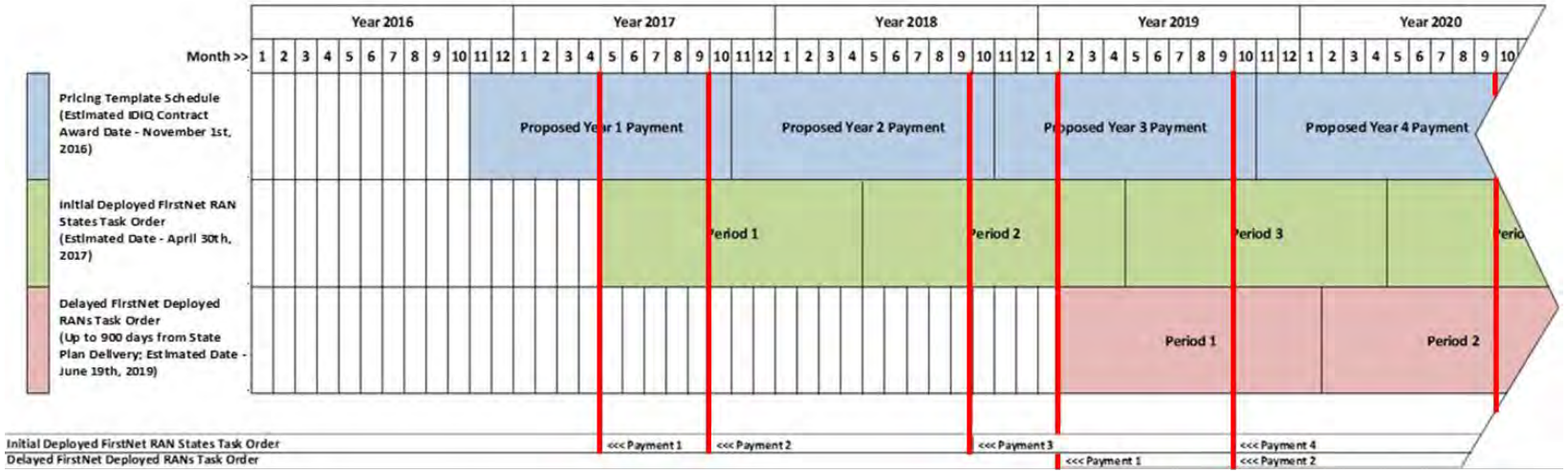


Figure 1 Notional Contracting Process – Initial Years of IDIQ Contract

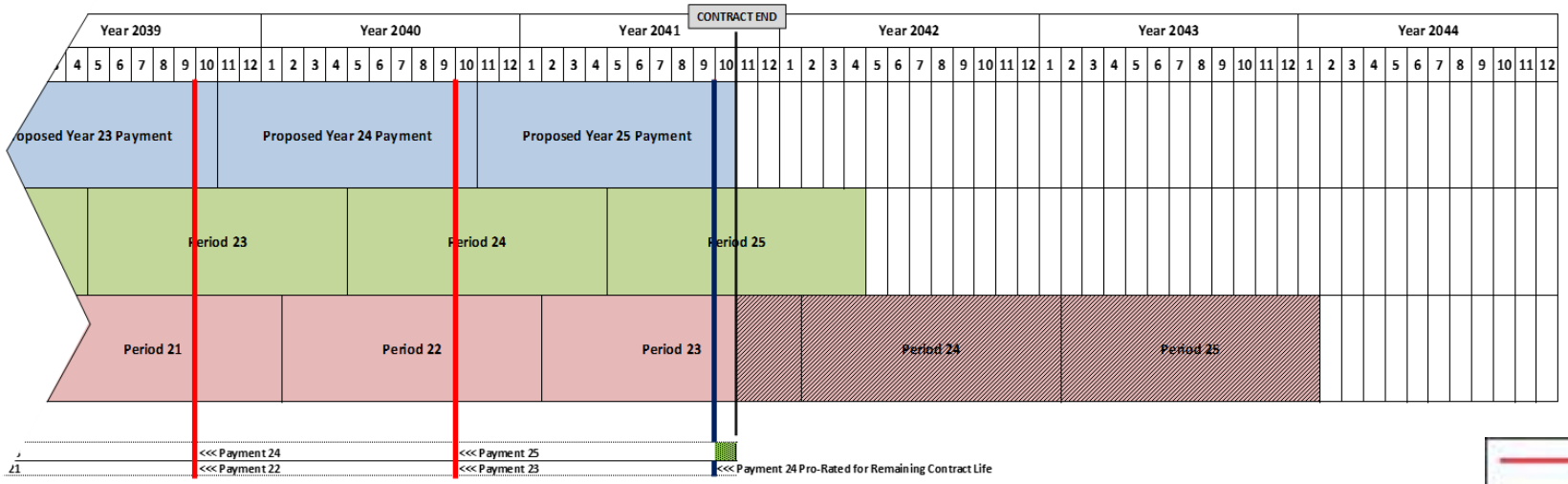


Figure 2 Notional Contracting Process – Final Years of IDIQ Contract

* Government fiscal years begin October 1st each year.

L.3.3.5 Gross FirstNet Value

The Offeror shall provide its estimated gross FirstNet value for each of the 56 states and territories. This gross FirstNet value represents all revenues (on a cash basis) that the Offeror expects to be generated by being awarded the NPSBN contract, inclusive of revenues derived from public safety use, revenues from excess network capacity, and all other revenues that the Offeror projects. Gross FirstNet value shall not include the cash identified as payments to the Contractor in Section L.3.3.2, Payments to the Contractor.

L.3.3.6 State-Specific Costs

The Offeror shall provide its estimated total projected costs (on a cash basis) incurred through the FirstNet program for each of the 56 states and territories in the appropriate worksheet in the template. These costs are defined as cash costs to deploy, maintain, and operate the state or territory's respective RAN, as well as any other state-specific cash costs, but exclude payments to FirstNet. These costs do not include any costs related to the Day 1 task orders described in Section B, Supplies or Services and Prices/Costs, Section B.2.1, Day 1 Task Orders.

L.3.3.7 FirstNet Minimum Payment Thresholds

The minimum payment thresholds represent the annual payments required for FirstNet's financial sustainability, establishing a network reserve fund, supporting recapitalization of the network, and other authorized purposes. Refer to Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet

Operational Sustainability, for the minimum payment thresholds by fiscal year. As such, the Offeror's payments to FirstNet must be at least equal to FirstNet's required minimum payment thresholds outlined in Table 1 of Section B, though the Offeror may propose payments above the minimum payment thresholds.

The proposed payments to FirstNet may differ in each Government fiscal year but must be fixed and established based on the Offeror's proposed technical solution throughout the life of the contract and in taggregate (total payments to FirstNet) must meet, and may exceed, the minimum payment thresholds in every year.

L.3.3.8 Net Present Value Assumption

Payments to FirstNet will be discounted to the present value using the 20-year Treasury bond (available at https://www.treasury.gov/resource-center/data-chart-center/interest-rates/Pages/TextView.aspx?data=yield) as published at 5:00 p.m. Eastern Time the day of the release of this RFP.

L.3.3.9 Re-Pricing of Payments to FirstNet and Re-Propose Solution

The Offeror shall propose payments to FirstNet no less than the minimum payment thresholds as described in Section L.3.3.7, FirstNet Minimum Payment Thresholds. Following adjustment of the payments to FirstNet—positive or negative, as applicable—to reflect states and territories that assume responsibility for deploying their own RAN, if the adjusted payments to FirstNet fall below the minimum payment thresholds described in Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet Operational Sustainability, the Contractor will be permitted to revise its proposal, including its payments to FirstNet.

Table of Contents

M Evaluation Factors for Award

M.1 General Information

Proposals shall be prepared in accordance with and comply with the requirements and instructions contained in this Request for Proposal (RFP). Each proposal will be evaluated against the evaluation factors identified herein. The details on the complete evaluation process are outlined in M.2, Evaluation Process.

M.2 Evaluation Process

In accordance with Federal Acquisition Regulation (FAR) 15.202 and as described herein, a multi-phased approach will be used to determine the overall best value to the Government for this acquisition. Each proposal will be reviewed and evaluated in accordance with its contents; the Government will make no assumptions related to the Offeror's performance that the Offeror does not specify in its proposal.

In light of the First Responder Network Authority's (FirstNet) objective-based acquisition approach and the unique nature of the FirstNet program and the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), the Government will consider unique, innovative approaches to achieving an overall best value solution consistent with the objectives as set forth in Section C, Statement of Objectives (SOO) and the requirements and recommendations specified in Section J, Attachment J-3, FCC TAB RMTR. The Government will consider any and all proposed solutions utilizing emerging technologies and/or non-traditional practices or solutions with regard to the overall Nationwide Public Safety Broadband Network (NPSBN) in accordance with the terms and conditions, instructions, and evaluation criteria as stated herein.

Any exceptions or deviations by the Offeror to the terms and conditions stated in the Offeror's proposal for inclusion in the resulting contract may make the offer unacceptable for award without discussions. If an Offeror proposes exceptions to the terms and conditions of this RFP, the Government may make an award, without discussions, to another Offeror that did not take exception to the terms and conditions, if such Offeror is determined to be the best overall value for this effort.

As part of the multi-phased approach, the Government reserves the right to request Offerors to conduct oral presentations and/or technical demonstrations as a result of this RFP. Those Offerors will be notified and provided any additional information and instructions, as necessary, regarding oral presentations and/or technical demonstrations.

The Day 1 task order evaluations will *not* be conducted separately from the evaluation of the overall NPSBN proposed solution as they make up specific portions of the NPSBN solution, based on the SOO (Section C) and associated attachments in Section J.

M.2.1 Phase I – Capability Statements

For Phase I of the multi-phased approach, interested parties should demonstrate they are capable of performing the work by providing a capability statement (see FAR Part 15.202 and Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.2.4, Submission of Capability Statements, for instructions). Following review and evaluation of all capability statements received as a result of this phase, those deemed best qualified based on the evaluation criteria stated herein will be

invited to submit a proposal in accordance with the instructions contained in Section L, Instructions, Conditions, and Notices to Offerors or Respondents.

Notifications will be issued to *all* Offerors that submit a capability statement as a result of this RFP. Each notification will include feedback regarding evaluation of the capability statement that identifies strengths and/or weaknesses that shows whether the company is or is not, based on the capability statement review and evaluations, considered a viable competitor.

Capability statements will be evaluated based on the following criteria, which are of equal importance:

- **Public safety use and adoption of the NPSBN** – Offerors will be evaluated based on their demonstration of their ability to successfully drive adoption and use of the NPSBN by public safety users.
- **Nationwide coverage and capacity** – Offerors will be evaluated based on their demonstration of their ability to provide Band 14 and non-Band 14 coverage and capacity in each of the 56 states and territories, including rural and non-rural areas.
- **Rural partnerships** – Offerors will be evaluated based on their demonstration of their existing and planned partnerships with rural telecommunications providers, including commercial mobile providers, utilizing existing infrastructure to the maximum extent economically desirable to speed deployment in rural areas.
- **Ability to monetize network capacity** – Offerors will be evaluated based on their strategy and demonstration of their ability to monetize network capacity, which may include a secondary user customer base and sales/distribution channels to reach primary and secondary users.
- **Financial sustainability** – Offerors will be evaluated based on their demonstrated approach and financial sustainability. Additionally, Offerors' financial stability will be evaluated in regard to their ability to develop, implement, sustain, and enhance the NPSBN based on the Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones set out in Section J, Attachment J-8, IOC/FOC Target Timeline.

M.2.2 Phase II – Solicitation Conformance

During this phase, the Government will conduct an initial review of the proposals received in order to verify conformance and completeness with the RFP instructions, including any/all attachments and exhibits, prior to commencement of evaluations as stated herein in Section M.2.3, Phase III – Pass/Fail, and Section M.2.4, Phase IV – Detailed Evaluation.

This conformity review will consist of verification that all documentation has been provided in accordance with Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3, Proposal Format and Submission Instructions. The Government will also utilize the Section J, Attachment J-22, Solicitation Conformance Traceability Matrix (SCTM), in order to make a determination regarding completeness.

Failure to submit any information and/or documentation as stated in this RFP and as listed on the SCTM may result in the proposal submission being removed from any further consideration.

M.2.3 Phase III – Pass/Fail

During this phase, the Government will review and evaluate each proposal to ensure it meets the pass/fail factors identified herein. The following pass/fail factors will be evaluated based on the criteria

as stated herein. Failure to pass any of these factors may result in the proposal submission being removed from any further consideration.

M.2.3.1 FirstNet Minimum Payment Thresholds

Offerors shall complete Section J, Attachment J-13, Pricing Template, to demonstrate its ability to sustain the annual payments to FirstNet for the life of the contract. Offerors' proposed payments to FirstNet shall be disbursed on an annual basis and shall not be less than the minimum payment thresholds described in Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet Operational Sustainability. Payments to FirstNet must be submitted for each of the 56 states and territories. For this phase, the Offeror must demonstrate its ability to meet the minimum payment thresholds. The minimum payment is evaluated based on the sum of the payments proposed for all 56 states and territories for each contract year without regard to the Net Present Value (NPV) calculation (see Section M.4.5.1, Net Present Value of Payments to FirstNet).

M.2.3.2 Rural Partners and Subcontractors

Offerors shall complete Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, to demonstrate their ability to meet the objective to provide coverage in each of the 56 states and territories and to ensure that rural coverage includes partnerships with rural telecommunications providers. The Offeror's solution must demonstrate commitment to exercise rural telecommunications provider partnerships for at least 15 percent of the total rural coverage area nationwide at FOC. While Attachment J-2 requests these data by states, the 15 percent coverage factor will be evaluated on a nationwide basis only for this phase.

M.2.4 Phase IV – Detailed Evaluation

Those Offerors whose proposed solutions have been determined to conform to the RFP in Phase II and successfully pass Phase III will move into Phase IV. During this phase, the Government will commence the detailed evaluation of all information and documentation received from the Offerors based on the evaluation factors as stated herein.

The Government may consider, as part of its evaluation, any oral presentations and/or technical demonstrations or other discussions and publicly available materials gathered as part of the Government's evaluation. All of these materials may be used as part of the evaluation of the Offeror's ability to meet the objectives stated in Section C, SOO.

M.3 Basis for Award

Contract award shall be made to the responsible Offeror whose offer, in conforming to this RFP, provides the overall best value to the Government, when all evaluation factors are considered. All evaluation factors, when combined, are significantly more important than the value proposition. The Government may conduct a trade-off analysis and make an award to other than the highest technically rated Offeror or other than the Offeror presenting the most favorable value proposition. Due to the unique nature of FirstNet and the NPSBN, rather than conduct a *traditional* trade-off analysis where the Government typically considers price and non-price factors, the trade-off analysis for this acquisition will utilize the results of a value proposition assessment (see Section M.4.5) and non-price factors to determine the overall best value solution.

The Government reserves the right to *not* make an award as a result of this competition if, in the opinion of the Government, none of the submissions would provide satisfactory performance that is

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

considered fair and reasonable and/or economically feasible in the Government's sole determination. Additionally, the Government reserves the right to remove an Offeror's proposed solution from further consideration if it is determined to be unacceptable in any of the evaluation factors and/or sub-factors.

M.4 Evaluation Factors

The evaluation will consist of a determination and analysis of strengths, weaknesses, and risks of each proposed solution. Risk will be included in the evaluation of each factor (and/or sub-factors) and will not be evaluated as a separate factor. The Government may consider all proposal information submitted when assessing risk. The Offeror will be evaluated based on its demonstration and understanding of the objectives, including demonstrated creativity and thoroughness in its proposed solution. The Government may consider all proposal information submitted and presented pertaining to the Offeror's proposed solution when conducting the evaluation and determining overall best value.

The following evaluation factors will be utilized in order to determine which Offeror provides the best overall value. Evaluation factors are comprised of Business Management (Section M.4.1), Coverage and Capacity (Section M.4.2), Products and Architecture (Section M.4.3), the Offeror's Past Performance (Section M.4.4), and the Offeror's Value Proposition Assessment (Section M.4.5).

Evaluation factors are listed in descending order of importance:

- Business Management is more important than Coverage and Capacity.
- Coverage and Capacity and Products and Architecture are of equal importance.
- Business Management, Coverage and Capacity, and Products and Architecture combined are more important than the Volume III – Offeror's Value Proposition Assessment.
- The Volume III – Offeror's Value Proposition Assessment is more important than Past Performance.

Sub-factors for any of the evaluation factors are of equal importance unless otherwise stated.

M.4.1 Volume I – Business Management Factor

The Offeror will be evaluated based on its understanding of the effort, including innovation, creativity, and thoroughness shown in addressing the objectives (Section C, SOO) and applicable Section J attachments. The Government will evaluate the Offeror's business management approach to providing effective management of its delivery, operation, and maintenance of the NPSBN. The proposed approach will be evaluated to determine the extent to which it demonstrates a comprehensive, sound, efficient, and realistic approach to managing and ensuring successful contract performance within time and budget constraints.

The Business Management Factor includes evaluation in the following sub-factors:

- General
- Leadership and program management
- Public safety customer acquisition
- Customer care and life-cycle sustainment
- Offeror financial sustainability
- Delivery mechanism for state plans
- Quality Assurance Surveillance Plan
- Deliverables table

M.4.1.1 Section One – General

The Offeror's proposed solution will be evaluated based on the following elements:

- Small business subcontracting plan – This shall be evaluated pursuant to FAR Part 19.705.
- Contractor responsibility information – This shall be evaluated pursuant to FAR 9.104 in order to determine a prospective Contractor's determination of responsibility.
- Past performance – This shall be evaluated in accordance with Section M.4.4, Past Performance Factor.
- Offeror's experience – This shall be evaluated based on any proposed experience with regard to the Offeror's solution for the NPSBN to include the Offeror's proposed structure and experience of the subcontractors/teaming partners, the relationship between the Offeror and these organizations, and their combined ability to support the proposed solution with innovative approaches.

M.4.1.2 Section Two – Leadership and Program Management

The Offeror's solution must demonstrate its ability and proposed approach regarding leadership and program management. This will be evaluated based on the Offeror's proposed management plan and approach to achieving its stated solution, which demonstrates the following elements:

- Solution to ensure the services meet objectives in Section C, SOO
- Overall staffing plan for the NPSBN, including any proposed teaming arrangements and/or subcontractors
- Integrated Master Schedule and Work Breakdown Structure that encompass build-out and transition-to-operations activities with respect to the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline
- Details of existing 3rd Generation Partnership Project (3GPP) standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its proposed teaming partners and/or subcontractors
- Solution to leverage existing commercial and/or other infrastructure

The Offeror's proposed solution will also be evaluated based on its approach pertaining to:

- Corporate-level organizational structure, including the teaming/subcontracting roles and responsibilities as they relate to the NPSBN
- Comprehensive program management reflecting the Offeror's ability to provide seamless, efficient management of the NPSBN over the life of the contract and any subsequent task orders
- Supporting and facilitating FirstNet's compliance with the Act and other applicable local, state, tribal, and federal legislation (including, for example, the National Environmental Policy Act [NEPA], and the Communications Act)
- Organizational structure, staffing plan, and qualifications and experience of key personnel and executive leadership that will support the FirstNet program

M.4.1.3 Section Three – Public Safety Customer Acquisition

The Offeror must propose an approach to satisfy FirstNet's public safety customer acquisition objectives. This sub-factor will evaluate the Offeror's proposed public safety device connection targets (connection targets), which represent its anticipated number of public safety device connections

(primary users and extended primary users) by each of the 56 states and territories over the life of the contract, as detailed in Section L, Instructions, Conditions, and Notices to Offerors or Respondents. The Offeror's proposed connection targets will be evaluated relative to the estimated current demand at a state and territory level for the primary user group, as well as the extended primary user group as identified in Section J, Attachment J-24, Public Safety Device Connections Template.

This sub-factor will also evaluate the Offeror's proposed strategy to minimize time required to provide broadband services to public safety. This includes the Offeror's current sales and marketing structure, proposed go-to-market strategy for adoption, and nationwide sales and marketing plan to drive widespread adoption of FirstNet priority- and preemption-capable products and services by public safety users. Preference in the evaluation will be placed on adoption by primary users.

The Offeror's proposed solution will be evaluated based on its approach pertaining to:

- Connection targets
- Go-to-market strategy to sell and market services, including priority and preemption, to public safety users, including pricing and incentive programs
- Marketing of an applications ecosystem
- Description and staffing of the marketing and sales organization(s) tasked to support the NPSBN, including the proposed strategy and approach to ensure strategic alignment and mitigation of sales and marketing channel conflict among teaming partners to ensure adoption and use of the NPSBN
- Ability to meet current, emerging, and future customer needs and standards, including a device portfolio and estimated price points

M.4.1.4 Section Four – Customer Care and Life-Cycle Sustainment

The Offeror's proposed approach must demonstrate its ability to satisfy customer care and life-cycle innovation as stated in Section C, SOO. This sub-factor will be evaluated based on the Offeror's proposed ability to demonstrate that its solution will deliver provisioning capabilities, and solution for service and delivery, including all linkages to sales, fulfillment, and customer care. Additionally, the Offeror's solution will be evaluated based on the proposed billing management capabilities and proposed management approach.

The Offeror's proposed solution will be evaluated based on its approach pertaining to:

- Performance monitoring and reporting for devices/network equipment, services, and customer care, including providing subscribers with activation, repair, technical assistance, replacement devices, and emergency restoration support
- Metrics to monitor customer satisfaction, the service levels reported by current customers, and the solution for maintaining or improving these service levels over the 25-year period of performance
- Customer care strategy to minimize churn and promote customer retention among public safety users
- Current billing support services for broadband and wireless services and any current public safety services throughout the FirstNet service area

M.4.1.5 Section Five – Offeror Financial Sustainability

The Offeror's proposed approach must demonstrate its ability to satisfy financial sustainability requirements. This section will be evaluated based on the Offeror's solution regarding its financial robustness to develop, implement, sustain, and enhance the NPSBN within the time frames, duration, and objectives set out in this RFP.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

The Offeror's proposed solution will be evaluated based on the following aspects:

- Financial statements of the Offeror in order to demonstrate financial stability and capacity
- Details of source funding or financing to support the NPSBN
- Terms of any parent company or other guarantees
- Financial forecasts and how the Offeror proposes to commercialize the excess network capacity

M.4.1.6 Section Six – Delivery Mechanism for State Plans

In accordance with the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), upon completion of the RFP process, FirstNet must present a plan to the governor of each state and territory that includes, among other things, "… details of the proposed plan for buildout of the nationwide interoperable, broadband network in such State."

It is FirstNet's intent to deliver these plans using an online, interactive tool. The Offeror's proposed solution will be evaluated on the following aspects:

- Readability, navigability, organization, and other pertinent aspects of the user interface design
- Ability to support the objectives outlined in Section J, Attachment J-18, Delivery Mechanism Objectives for State Plans
- Technical design and system adaptability and security

M.4.1.7 Section Seven – Quality Assurance Surveillance Plan

The Offeror will be evaluated on its proposed Quality Assurance Surveillance Plan and the extent to which it accurately monitors and communicates to FirstNet the contractual, operational, financial, and technical performance of the NPSBN.

M.4.1.8 Section Eight – Deliverables Table

The Offeror's proposed deliverables will be evaluated based on its ability to demonstrate industry best practices and professional expertise as well as the alignment with the proposed performance metrics/standards defined in the Offeror's Quality Assurance Surveillance Plan (Section J, Attachment J-9, QASP Surveillance Matrix Template).

M.4.2 Volume II – Coverage and Capacity Factor

The Offeror's proposed solution will be evaluated based on its ability to provide coverage and capacity solutions as described in the sub-factors below. Coverage propagation and geographic information system tools will be utilized to assist in the evaluation process. These tools include but are not limited to MapInfo 11 and ArcGIS. This factor will be evaluated based on both a quantitative and qualitative perspective. The coverage and capacity factor includes evaluation in the following sub-factors:

- Coverage and Capacity Maps and Statistics
- Radio Access Network (RAN) Strategy and Solutions
- IOC Milestones for Coverage and Capacity

M.4.2.1 Coverage and Capacity Maps and Statistics

The Government will evaluate this sub-factor utilizing a quantitative approach. The Offeror's proposed solution will be evaluated for each of the 56 states and territories using the information provided by the Offeror through coverage maps as well as network statistics included in Section J, Attachment J-17,

Coverage and Capacity Template. The Government will evaluate the maps and statistics against the coverage objectives specified in Section J, Attachment J-1, Coverage and Capacity Definitions. For the coverage maps, each individual grid block will be assessed for meeting the definition of coverage (see Section J, Attachment J-1, Coverage and Capacity Definitions). Only those grid blocks that have a reasonable amount of coverage will be considered acceptable. As noted in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.1.2.2, Network Planning and Design, detailed site locations are not required; however, for evaluation purposes, the Government reserves the right to request detailed site information (to include all site data for up to two counties per state or territory.) If requested, these data are to be supplied using the "Site Summary" tab in Section J, Attachment J-17, Coverage and Capacity Template.

The Government will evaluate the Offeror's proposed solution using a quantitative approach for each of the following coverage and capacity elements, which are of equal importance:

- **Non-Band 14 Area Coverage** – The amount of land mass that is covered with non-Band 14 coverage solutions
- **Non-Band 14 Population Coverage** – The amount of population that is covered with non-Band 14 coverage solutions
- **Band 14 Area Coverage** – The amount of land mass that is covered with Band 14 coverage solutions
- **Band 14 Population Coverage** – The amount of population that is covered with Band 14 coverage solutions
- **Band 14 Network Capacity** – The amount of designed network capacity for first responders and secondary users

M.4.2.2 RAN Strategy and Solutions

The Offeror's proposed solution will be evaluated qualitatively based on the proposed RAN design solution, which must include architecture, functionality, design, implementation, roadmap, and operational strategies that effectively use resources, skillsets, an organizational structure, and tools.

M.4.2.3 IOC Milestones for Coverage and Capacity

The Offeror's proposed solution will be evaluated qualitatively based on the proposed approach to meeting and/or exceeding the deployment schedule in accordance with the coverage and capacity milestones as provided in Section J, Attachment J-8, IOC/FOC Target Timeline.

M.4.3 Volume II – Products and Architecture Factor

The Offeror's solution will be evaluated based on its proposed approach, including innovation, creativity, and thoroughness, shown in planned execution of the overall objectives as stated in Section C, SOO, and associated Section J attachments as applicable. The products and architecture factor includes evaluation of the Offeror's proposed solution in the following sub-factors:

- Services
- Applications
- Device Ecosystem
- Architecture and Infrastructure
- Operations
- Security
- Test Strategy

M.4.3.1 Services

M.4.3.1.1 Basic Network Services

The Offeror will be evaluated based on its proposed solution to enable basic network services, including but not limited to messaging, streaming services, voice telephony, machine-to-machine, Next Generation 9-1-1, lawful intercept, Wireless Emergency Alerts, and basic data for the NPSBN. The Offeror should outline its approach based on each of the IOC/FOC milestones and compliance with 3GPP or relevant international standards.

M.4.3.1.2 Quality of Service, Priority, and Preemption

The Offeror will be evaluated on its proposed solution for Quality of Service, Priority, and Preemption (QPP) and service readiness in the event of an emergency and/or network congestion. The Offeror will be evaluated on its proposed solution (including systems, interfaces, and settings) pertaining to QPP states (static, dynamic, controlled), Covered Leasing Agreement (CLA) user-states (free range, restricted, pre-empted), emergency states (user type and role), QPP profiles and static user data (default and emergency QPP profiles for different users with different roles), dynamic data (user location, user operational status, incident role, incident identifier, incident location, and incident severity), QPP application profiles, group of application profiles into operational profiles for an agency, dynamic QPP management, and end-to-end Quality of Service and Priority for public safety users. The Offeror will be evaluated on its proposed solution of a dynamic controller.

M.4.3.1.3 Identity, Credential, and Access Management

The Offeror will be evaluated based on its proposed solution pertaining to Identity, Credential, and Access Management (ICAM) within the following elements:

- **Federated Identity Management** – The Offeror's ability to support federated identity management, allowing users of one agency to access data and services provided by a different agency, including evaluation of the proposed federated identity interfaces that the solution supports and any impacts on an existing agency's infrastructure and legacy applications that an agency exposes.
- **Identity Proofing and Onboarding** – The Offeror's ability to support agencies being properly onboarded to leverage the FirstNet ICAM solution, including identifying proofing of users and ensuring the agency is in compliance with security parameters (additional details available in Section J, Attachment J-10, Cybersecurity). The Offeror's proposed timelines and processes for onboarding and certifying an agency and identity-proofing users will be considered. This will include the proposed process for addressing agencies that lack a compliant identity proofing and onboarding solution/process (i.e., Identity-as-a-Service).
- **Credential Management** – The Offeror's ability to support credential management, including ensuring credentials are secure and align with the specifications in Section J, Attachment J-4, System and Standard Views, including but not limited to the management of user attributes and access policies that enable interoperability between agencies.
- **Single Sign On and Authentication** – The Offeror's ability to support effective, efficient, realistic, and secure methods for public safety users to authenticate, including but not limited to authentication into devices, mobile applications, Web applications, and desktop applications.
- **Authorization** – The Offeror's ability to support dynamic access management and the manner in which its solution will easily enable applications to authorize users before granting access to the

application or data, including but not limited to how static and dynamic access policies are created, managed, and applied to applications, services, and resources.

M.4.3.1.4 Mission-Critical Services

The Offeror will be evaluated based on its proposed approach regarding the design and plans for mission-critical Push-to-Talk, data, voice, proximity services, and location services for each IOC/FOC milestone, including its compliance with relevant international standards.

M.4.3.2 Applications

The Offeror will be evaluated based on its proposed solution to execute an applications ecosystem, as defined in Section M.4.3.2.1, Applications Ecosystem. This will include demonstrating its ability to provide an applications ecosystem that supports the NPSBN with capabilities and services relevant to public safety. This will include its proposed solution to provide an ecosystem that includes, at a minimum, an evolving portfolio of mobile, enterprise, cloud services, and applications; an applications development platform; a vibrant application developer community; a FirstNet applications store; local control of users, subscriptions, services, and applications; federation of identity management, data, applications, and resource sharing across diverse public safety agencies; Core service and application delivery platforms; data and applications security; and privacy compliance across local, state, regional, tribal, and federal users.

In addition, this sub-factor includes evaluation of the Offeror's proposed solution within the following elements:

- Applications ecosystem
- Offeror-provided applications

M.4.3.2.1 Applications Ecosystem

The Offeror's proposed solution for the applications ecosystem will be evaluated based on the service delivery platform, application development platform, hosting and cloud services, FirstNet applications store, application life-cycle management, developer and application certification, and application security described.

M.4.3.2.1.1 Service Delivery Platform

The Offeror's proposed solution will be evaluated based on its operational capabilities, which includes gateway policy (i.e., authorization, privacy, throttling, and quotas), security, Application Programming Interfaces (APIs) middleware, and transformation to back-end network service platforms. Additionally, this will include the Offeror's proposed approach regarding its ability to orchestrate one or more network services with an application consuming these APIs, as well as for first responders handling responder emergencies and immediate peril events.

M.4.3.2.1.2 Application Development Platform

The Offeror's proposed solution will be evaluated based on how it supports, allows, and facilitates rapid and innovative third-party public safety application development. In addition, the Offeror's roadmap for creating a vibrant application developer community will be evaluated.

M.4.3.2.1.3 Hosting and Cloud Services

The Offeror's proposed solution will be evaluated based on the extent to which its cloud services solution provides the necessary service redundancy, resiliency, and contingency capabilities to ensure service availability. This includes the analysis of proposed offerings for Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) solutions, as well as data analytics, storage services, and analytics platform.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

M.4.3.2.1.4 FirstNet Applications Store

The Offeror will be evaluated based on its solution and demonstrated approach for supporting a FirstNet applications store, including how the applications store provides public safety agencies and users with a cost-effective, easy method to access secure, value-added public safety applications. The evaluation will include assessing a client's ability to search, browse, sort, select, download, purchase, review, and rate applications. The evaluation will include an assessment of the proposed approach for the application developers' registration process, ease of application publishing and management, application version control, and application monetization and settlements methods.

M.4.3.2.1.5 Application Life-Cycle Management

The Offeror's proposed solution will be evaluated based upon its ability to demonstrate knowledge of application life-cycle management processes, including governance, development, deployment, and operations. This will also include an assessment of the proposed approach for how applications are created based on various categories (e.g., mobile, enterprise, desktop), tested, deployed, updated, monitored, and deprecated.

M.4.3.2.1.6 Developer and Application Certification

The Offeror's proposed solution will be evaluated based on its approach to developing a timely and effective solution for certifying application developers and public safety applications as a means to ensure the applications function as expected and are secure, resilient, scalable, and free from malware and unintended behavior. This will include a detailed analysis of the Offeror's approach pertaining to the processes and criteria for certifying application developers and certifying applications. Additionally, the evaluation will include an assessment of the proposed approach for both newly developed and existing public safety applications and how they are handled and certified.

M.4.3.2.1.7 Application Security

The Offeror's proposed solution will be evaluated based on its approach regarding security of the application layer and the data associated with users. This will include an assessment of the proposed solution regarding data protection against unauthorized access and maximizing privacy, data integrity, and data availability in end-to-end scenarios. Additionally, this evaluation will include an assessment of the Offeror's ability to enable the secure coexistence of certified FirstNet and commercial applications on a device. This will include evaluation pertaining to the approach for data and applications security monitoring, alerting, and mitigation for ongoing security operations.

M.4.3.2.2 Offeror-Provided Applications

The Offeror will be evaluated based on its proposed solution for demonstrating its understanding of the effort, including innovation, creativity, and thoroughness of providing the specific applications described below.

M.4.3.2.2.1 Local Control Application

The Offeror's proposed solution will be evaluated for providing direct and indirect control of the NPSBN to Public Safety Entities (PSEs) through local control. Local control is a set of features that allows a PSE to affect direct change over the operational and administrative characteristics of the NPSBN for its users as well as a set of business processes that provides the PSE indirect input into operational aspects of the NPSBN that affect its users. Details can be found in Section L, Instructions, Notices, and Conditions to Offerors or Respondents, Section L.3.2.2.2.2.1, Local Control Application.

M.4.3.2.2.2 Public Safety Entity Home Page

The Offeror's proposed solution for providing a PSE home page will be evaluated. The home page will provide a central point of access to information about the NPSBN as well as to other applications and information, such as the local control application, news and weather information of interest to the PSE, and link(s) to the customer-facing, Web-based portal. Details can be found in Section L, Instructions, Notices, and Conditions to Offerors or Respondents, Section L.3.2.2.2.2.2, Public Safety Entity Home Page.

M.4.3.3 Device Ecosystem

The Offeror's proposed solution pertaining to the device ecosystem will be evaluated based on a robust device portfolio and its roadmap. This will include the proposed approach to provide the necessary certifications and support.

In addition, this sub-factor includes evaluation of the Offeror's proposed solution within the following elements:

- Management of the Universal Integrated Circuit Card (UICC) SIM types that automatically support all partner and roaming network(s) and the life-cycle support of the profile(s). Devices that can operate across multiple networks with a single UICC are preferable.
- Support of a standards-compliant Device Management client.
- Device approval process, including Federal Communications Commission (FCC) certification, Personal Communications Services (PCS) Type Certification Review Board (PTCRB) certification (including the waiver request process), FirstNet's Device Independent Verification and Validation (IV&V), and carrier acceptance for current and future devices.

M.4.3.3.1 Device Portfolio

The Offeror will be evaluated based on its proposed solution for providing a device portfolio and roadmap that supports Section C, SOO, and completion of Section J, Attachment J-11, Device Specification Template. The proposed solution will be evaluated based on the diversity of the portfolio across key device categories, the Offeror's ability to operate securely on the NPSBN and partner networks, and the ability to be interoperable with the FirstNet applications ecosystem. The proposed solution will also be evaluated based on the device ecosystem as a whole, its life-cycle management, and support for a variety of UICC configurations, accessories, a Bring Your Own Device (BYOD) ownership model, and Mobile Device Management (MDM).

M.4.3.3.2 Band 14 Devices

The Offeror's solution will be evaluated on the proposed approach to provide a Band 14-capable device portfolio and roadmap(s), including but not limited to portables, modems, in-vehicle routers, Vehicular Network Systems, and Machine to Machine (M2M) or Internet of Things (IoT) configurations. The Offeror will also be evaluated on the management ecosystem strategy for devices, including device management and application management and security, as well as the portfolio approach based on each IOC/FOC milestone and compliance with 3GPP or other relevant international standards.

M.4.3.3.3 Universal Integrated Circuit Card Management

The Offeror will be evaluated on its proposed solution for the management of the UICC and the life-cycle support of the profile(s). Devices that can operate across multiple networks with a single UICC are preferable.

M.4.3.3.4 Device Management Client

The Offeror will be evaluated on its proposed solution for support of a standards-compliant device management client.

M.4.3.3.5 Device Approval Process

The Offeror's proposed solution will be evaluated based on its demonstrated ability to provide details of its device approval process, including FCC certification, PTCRB certification (including the waiver request process), FirstNet's Device IV&V, and commercial carrier acceptance for current and future devices.

M.4.3.4 Architecture and Infrastructure

The Offeror will be evaluated on its proposed NPSBN network architecture solution comprising the nationwide Core network architecture, state integration plans, transmission systems, and interconnection and interworking.

M.4.3.4.1 Nationwide Core Network Architecture and State Integration

The Offeror will be evaluated on its proposed NPSBN network architecture solution comprising the following areas for each IOC/FOC milestone:

- Logical architecture regarding system and architecture views for all user and control planes for the NPSBN
- Integration of secondary users without impacting public safety users and services
- Services to public safety users
- Key Core network locations used for the NPSBN
- Network specifications, design criteria, service quality, and operational metrics of the Offeror's solution
- Session continuity between the NPSBN and other networks
- Roaming strategy pertaining to support of roaming with other wireless networks
- Integration of roaming partners, ensuring seamless wireless services throughout the coverage footprint for public safety users, to include an outline demonstrating the proposed approach for integration of rural telecommunications providers
- Internet Protocol (IP) address assignments in the NPSBN and interworking with other networks
- Heterogeneous network integration, including the proposed strategy regarding integration of wireless technologies (e.g., Wi-Fi, small cells, distributed antenna solutions) into the NPSBN to form a seamless network implementation and operation

M.4.3.4.2 Transmission Systems Strategy

The Offeror will be evaluated on its ability to provide a transmission systems approach supporting RAN backhaul, backhaul aggregation, and a nationwide backbone transmission system for each IOC/FOC milestone. Specifically, the Offeror will be evaluated on its proposed solution in the following areas:

- RAN backhaul architecture, topology, and synchronization approach for its RAN solution

- RAN backhaul system aggregation transport network approach
- National transmission network approach
- End-to-end security of the transport network
- Routing and Diameter Routing Agent (DRA) approach for the user and signaling plane traffic on the NPSBN
- Transport service prioritization to ensure the integrity of end-to-end services for public safety, specifically with regard to QPP

M.4.3.4.3 Interconnection and Interworking

The Offeror will be evaluated on its ability to provide a solution for the interconnection and interworking required to support a seamless and interoperable NPSBN. Specifically, the Offeror will be evaluated on its proposed solution in the following areas:

- Integration of state-deployed RANs with the NPSBN, including population locations detailing the function for each location at each of the 56 states and territories
- Public Safety Enterprise Network (PSEN) and Public Safety Answering Point (PSAP) integration in accordance with the FOC milestones
- Public Switched Telephone Network (PSTN), Internet Service Provider (ISP), and peering integration in accordance with each IOC/FOC milestone
- Public Land Mobile Network Number (PLMN) and roaming partner integration in accordance with each IOC/FOC milestone

M.4.3.4.4 Public Safety Grade

The Offeror will be evaluated on its proposed solution for ensuring a level of hardening and resiliency within the NPSBN that will be necessary for public safety services, especially in case of operational challenges that are expected during natural and man-made events. Specifically, the Offeror's proposed solution will be evaluated based on the following areas:

- Network reliability related to the Offeror's network design, and support for demonstrating how its solution consistently performs according to its specifications for each IOC/FOC milestone
- Network resiliency in order to maintain the restoration time specified in Section C, SOO, in the face of natural disasters, faults, and other challenges to normal operation for each IOC/FOC milestone
- Network redundancy in order to increase service availability through local and geo-redundancy solutions designed into the NPSBN for each IOC/FOC milestone
- Mitigation of environmental factors that may have an adverse effect on the NPSBN's performance
- Operational management—including preventative and proactive measures for maintenance, disaster support, and new technologies—which results in a continual improvement of network performance, services, and support of public safety users

M.4.3.4.5 Network Implementation

The Offeror will be evaluated on its network implementation solution comprising network integration strategy, design assumptions, naming and numbering strategies, and implementation approach. Specifically, the Offeror's proposed solution will be evaluated based on the following areas:

- Network integration with partner service providers at each IOC/FOC milestone

- Naming and identifying NPSBN network nodes to facilitate seamless network services implementation and operation at each IOC/FOC milestone
- NPSBN design assumptions at each IOC/FOC milestone
- Numbering/addressing schema for public safety devices
- Program approach and schedule for the implementation of the NPSBN, covering all IOC/FOC milestones
- Migration of public safety users from any temporary non-Band 14 network to the NPSBN as soon as the NPSBN is available in a region
- Mobile number portability to ensure public safety users do not change their phone numbers when migrating to the NPSBN

M.4.3.5 Operations

The Offeror's solution will be evaluated based on the proposed design, architecture, and approach regarding an effective and complete operational life-cycle model that is consistent with the Information Technology Infrastructure Library (ITIL®) or other commercial operational and testing plans for all aspects of the NPSBN. This model should include processes needed for day-to-day management of the network, reactive processes around incidents and national events, and proactive processes resulting in continual improvement of service availability. The areas of operations that follow will be evaluated for the Offeror's proposed solution.

M.4.3.5.1 Network and Service Operations

The Offeror will be evaluated on how its managed services in the following areas will meet the stated service availability objectives for the NPSBN, as identified in Section C, SOO, for all services and applications. These areas contain processes that focus on continuous service delivery and proactive operations of the NPSBN. The Offeror will also be evaluated based on its proposed solution for the following areas:

- Systems and processes to identify and resolve service degradation issues
- National Incident Management System (NIMS) processes and interfaces
- Release management processes
- Business continuity/disaster recovery management processes
- Availability management processes
- Change management processes
- Capacity management processes
- National and local support structure for network configuration, maintenance, and monitoring
- Procedures and protocols to support use of deployable assets for natural disasters and major events

M.4.3.5.2 Business and Operational Support Systems

The Offeror will be evaluated on how its business and operational support systems in the following areas will support meeting the stated service availability objective for the NPSBN, as identified in Section C, SOO, for all billing, operational, and provisioning support systems. Each of these areas should contain processes that focus on support of the user life-cycle on the NPSBN. The Offeror's proposed solution will be evaluated based on the following areas:

- Business and Operational Support Systems (B/OSS) infrastructure

- Network and Element Management Systems
- End-user and device provisioning and management systems
- Configuration management systems
- Billing system capability and flexibility in defining new profiles and billing
- Device management systems
- Subscriber management (customer relationship management) systems
- Asset management systems
- Trouble ticketing systems
- Workflow systems
- Data processing
- APIs available to government for creation of automated reports

M.4.3.5.3 Services Management Center

The Offeror's proposed solution will be evaluated based on its ability to provide an NPSBN Services Management Center that is effective in managing the following operational network and service verticals. Each of these areas should contain processes that focus on the surveillance and response of support staff and systems monitoring the NPSBN. The Offeror's proposed solution will be evaluated based on the following areas:

- Operational center(s) of excellence for management and reporting of NPSBN services (integrated into a single management framework)
- Event-based Element and Network Management System
- Appropriate surveillance and technical support staff
- Effective visibility and timely communication of network and service status
- Around-the-clock (24x7x365) visibility and management of network and service status
- Ongoing quality management and improvement framework for meeting and exceeding performance objectives

M.4.3.5.4 Service Availability

The Offeror's solution will be evaluated based on its proposed plan for providing a redundant network designed to operate during natural and man-made disasters necessary to meet the service availability objective in Section C, SOO.

M.4.3.6 Security

The Offeror's solution will be evaluated based on its proposed architecture, operational, and security testing plans for all aspects of the NPSBN.

M.4.3.6.1 Public Safety Security

The Offeror's solution will be evaluated based on its proposed approach as it pertains to usability, mission primacy, operational security, responder safety, reliability, resiliency, Health Insurance Portability and Accountability Act of 1996 (HIPAA) data protection, Criminal Justice Information Services (CJIS) data protection, payment card industry (PCI) data protection, end-to-end protection of data, privacy, authentication, multi-layer security, and public safety data protection.

M.4.3.6.2 Architecture Security

The Offeror's proposed solution will be evaluated based on its approach related to architectural security considerations as depicted in Section J, Attachment J-3, FCC TAB RMTR, 3GPP standards, GSM Association (GSMA) specifications, transport, external interfaces, end-to-end security management and logging, private encryption key management infrastructure (to include policies and practices), fraud prevention and revenue assurance, network address translation (NAT) support, protection between users, signaling storms, rogue or spoofed devices, heterogeneous network support, operational support system, Domain Name System (DNS) security, messaging security, IP Multimedia Subsystems security, business support system, mobile Virtual Private Network (VPN) support, business continuity and disaster recovery, IP infrastructure network elements, security hardening, cybersecurity governance model, cyber supply chain, training, insider threat mitigation, cloud environments, virtualization security, software-defined networking security, and Voice over IP (VoIP) spam. The Offeror's proposed solution will be evaluated based on the following areas pertaining to domains:

- RAN within a state or territory (either FirstNet- or state-deployed)
- Backhaul network (Enhanced Node Base station) to regional aggregation points
- Aggregation network (aggregation of traffic in a region)
- National transport networks (network connections to regional and national Core sites)
- Evolved Packet Core
- Business Support Systems
- Operational Support Systems
- Applications ecosystem
- IMS
- Value-added services
- Messaging services
- PSE network connectivity
- NPSBN cloud environments

M.4.3.6.3 Device Security

The Offeror's proposed solution will be evaluated based on its approach to device security for FirstNet users, including but not limited to secure operating system architecture, authentication of users and applications, embedded applications, MDM and Mobile Application Management (MAM) (PSE-managed whitelist/blacklist), digital signature of the applications, device security, and BYOD to include devices, applications, and/or wearables.

M.4.3.6.4 Applications Security

The Offeror's proposed solution will be evaluated based on its approach to application security, including but not limited to applications ecosystem security, API security, the application software development life-cycle, application security certification, application vulnerability management, application developer certification, user logging, end-to-end application, application-specific port monitoring and validation, application-device security, data loss prevention, and secure application coexistence.

M.4.3.6.5 Identity, Credential, and Access Management Security

The Offeror's proposed solution will be evaluated based on its approach to effectively provide ICAM with federated identify from PSENs, authorization, credentialing, and the following areas related to identity assurance:

- User to device
- Device to network (Long Term Evolution [LTE] authentication)
- Network to application (identity management)
- Network to PSE network (identity management)
- User to application (identity management)
- User to PSE network (identity management)

M.4.3.6.6 Cryptographic Employment

The Offeror's proposed solution will be evaluated based on its approach to mitigate attack vectors against the NPSBN's infrastructure and devices using encryption.

M.4.3.6.7 Public Safety Enterprise Network Security

The Offeror's proposed solution will be evaluated based on its approach to formulate minimum security standards for PSE networks to connect to the NPSBN.

M.4.3.6.8 Cybersecurity Life-Cycle

The Offeror's proposed solution will be evaluated based on its approach to security, including but not limited to identifying vulnerabilities and threats, determining risks arising from threats and vulnerabilities, prioritizing risks to determine which warrant associated controls to address threats or vulnerabilities, specifying and implementing controls to address or mitigate those threats and vulnerabilities, assessing the effectiveness of controls, and monitoring the security of the system.

M.4.3.6.9 Cybersecurity Systems Engineering

The Offeror's solution will be evaluated based on the proposed cybersecurity systems engineering plan and its approach to ensure sustained security for the NPSBN.

M.4.3.6.10 Risk Management

The Offeror's proposed solution will be evaluated based on its approach to address risk management considerations, including but not limited to a Risk Management Methodology that is executed continuously during the system's development life-cycle and during the life of the NPSBN (to include the use of National Institute of Standards and Technology Risk Management Framework and/or the ISO 27000 series). The Offeror's proposed Risk Management Methodology will be evaluated based on the following steps:

- Asset identification
- Risk impact analysis
- Threat assessment
- Risk mitigation
- Security control selection and deployment
- Risk mitigation operations and maintenance

M.4.3.6.11 Cybersecurity Incident Response

The Offeror's solution will be evaluated based on the proposed Cybersecurity Incident Response Plan.

M.4.3.6.12 Security Operations Center

The Offeror's proposed solution will be evaluated based on its approach in supporting the objectives of the security operations center, including but not limited to:

- Situational awareness that includes collecting, maintaining, and sharing information related to threats to network infrastructure, devices, data, and applications
- 24/7/365 cybersecurity monitoring of network infrastructure, devices, data, and applications
- Monitoring and analysis of user, system, and network access
- Assessment of system and data file integrity
- Establishment of the baseline network activity and utilization
- Recognition and analysis of activity patterns that are indicative of an incident or intrusion
- Analysis of logs for abnormal use patterns
- Information sharing and collaboration that integrates and disseminates information throughout the critical infrastructure partnership network
- Processing and posting suspicious activity reports
- Assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications
- Decision support that provides recommendations to partners and FirstNet leadership

M.4.3.6.13 Continuous Diagnostic Monitoring and Mitigation

The Offeror's solution will be evaluated based on the proposed approach to address hardware asset management, software asset management, vulnerability management, configuration settings management, continuous network and system monitoring, and mitigation strategies.

M.4.3.6.14 Cybersecurity Testing and Certification

The Offeror's proposed solution will be evaluated based on its approach related to cybersecurity testing and certification, including but not limited to:

- Testing life-cycle, including verification of security throughout the life-cycle of selection, procurement, integration, and operations support
- Testing methods to include assessment, testing, examination, and interviewing and associated processes and mechanisms to maintain testing results to ensure optimal accuracy and reproducibility
- Individual system validation
- Integrated configuration testing
- Independent applications/services testing for the following areas:
    - New applications at the national level
    - User-developed or state-developed applications
    - Upgrades to currently approved applications
    - Security patches to currently approved and fielded applications

M.4.3.6.15 Network and Configuration Management

The Offeror's proposed solution will be evaluated based on its approach related to network and configuration management, including:

- Network management
  - Configuration management
  - Configuration management planning and management
  - Configuration identification
  - Configuration control
  - Configuration status and accounting
  - Configuration verification and audit
- Vulnerability management
- Patch management
- Centralized security log management
- Security information and event management

M.4.3.6.16 Environmental and Physical Security

The Offeror's proposed solution will be evaluated based on its approach to environmental and physical security, including but not limited to power failure; humidity detection; cabinet door alarms; uninterruptable power supply (UPS) power failure; facility access control; monitoring and recording of activity within a facility to include egress/ingress (business/after hours and in restricted areas); heating, ventilation, and air conditioning (HVAC) failure or degradation; building door alarms; generator failure; low generator fuel; low battery; closed circuit television (CCTV) video surveillance systems; fire/smoke detection sensors; and protection from natural disasters (e.g., lightning/surge protection, water leak detection).

M.4.3.6.17 Information Security and Data Sensitivity

The Offeror's proposed solution will be evaluated based on its approach to information security and data sensitivity, including data in transit and data at rest. The Offeror's approach will be evaluated for its ability to protect, disseminate, and retain data.

M.4.3.7 Test Strategy

The Offeror's response will be evaluated based on its proposed architecture, design, and implementation of the NPSBN infrastructure to support the objectives (detailed in Section C, SOO) and FCC TAB requirements (detailed in Section J, Attachment J-3, FCC TAB RMTR), as well as the Offeror's ability to provide, demonstrate, verify, and measure aspects of the NPSBN test strategy identified but not limited to the areas specified in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.2.3, Test Strategy.

M.4.4 Past Performance Factor

The Offeror's proposed solution will be evaluated based on the following areas:

- History of successful completion of projects, especially those of similar size and/or scope, history of producing high-quality reports and other deliverables, and history of staying on schedule and within budget

- Quality of cooperation within the Offeror's organization and quality of cooperation and performance between the Offeror's organization and its customers
- Quality of service and improvement, as represented by the past performance data, and the approach to implementing performance measures and for improving system effectiveness over time
- Responsiveness to customers, as represented by past performance data, and success in responding to requests—both scheduled and ad hoc—for services, data, analysis, and additional tasks in a timely and appropriate manner
- Prior historical working relationship between the Offeror and the proposed subcontractors/teaming partners

In accordance with FAR 15.305(a)(2)(iv), in the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available via other sources, the Offeror may not be evaluated favorably or unfavorably as it relates to past performance.

M.4.5 Volume III – Offeror's Value Proposition Assessment

The Offeror's proposed solution will be evaluated based on its ability to meet all objectives, identified in Section C, SOO, and associated attachments in Section J, in exchange for revenues collected from Band 14 enabled public safety users and non-public safety users, use of available budget authority from FirstNet, and any other value-generating opportunities the Offeror can capitalize upon as a result of this contract.

M.4.5.1 Net Present Value of Payments to FirstNet

The NPV calculation of the nationwide (aggregated state and territory and nationwide) payments to FirstNet will be evaluated and utilized in conducting the best value trade-off analysis as described in Section M.3, Basis for Award. The NPV analysis will be conducted utilizing the data provided in the Payments to FirstNet worksheet of the Pricing Template contained in Section J, Attachment J-13. The NPV calculates the current value of a future stream of payments based on a defined interest rate. The Government will evaluate payments above the minimum payment thresholds.

Payments to FirstNet will be discounted to the present value using the 20-year Treasury bond (available at https://www.treasury.gov/resource-center/data-chart-center/interest-rates/Pages/TextView.aspx?data=yield) as published at 5:00 p.m. Eastern Time the day of the release of this RFP.

M.4.5.2 Offeror's Unbalanced and Unreasonable Value Determination

In place of a traditional pricing evaluation, the Government will evaluate the overall value proposition of the Offeror's pricing volume to determine if an unbalanced or unreasonable valuation exists. The overall value proposition is defined as all nationwide elements, which include the gross value, nationwide and state costs, budget authority, and proposed payments to FirstNet and to the Contractor over the life of the contract or in any given year. The Government will evaluate the overall value proposition for each contract year and for each of the 56 states and territories, which may include the aggregate of the entire period of performance (25 years) for the Offeror's proposed overall value proposition. A proposal that is determined to be unbalanced may be rejected if the Government determines that the lack of balance poses an unacceptable risk to the Government. Unbalanced or unreasonable pricing exists where the price of one or more nationwide or state elements is significantly overstated or understated despite an acceptable total overall value proposition.

The Government will perform a cost realism analysis of offers to (1) verify the Offeror's understanding of the requirements, (2) assess the degree to which proposed payments to the Contractor accurately reflect the effort described in the technical volume as it correlates to the IOC/FOC milestones, and (3) identify inconsistencies with specific objectives and associated attachments. The Contracting Officer reserves the right to limit these detailed analyses to proposals that have been evaluated as technically acceptable in Phases II and III of the multi-phased approach.

In addition, this evaluation will assess the proposed approach pertaining to the drawdown of the aggregate total of $6.5 billion of budget authority and the proposed payments to the Contractor for each IOC and FOC milestone, the nationwide Core, and each state and territory RAN, in accordance with the information stated in Section L, Instructions, Conditions, and Notices to Offerors or Respondents, Section L.3.3.2, Payments to the Contractor.

The information provided herein represents the Government's best effort to predict its needs for the objectives identified in this RFP. The Government reserves the right to evaluate any potential risk(s) and may perform a sensitivity analysis based on the overall proposed solution. This analysis may be used to identify and analyze any overall life-cycle expenses the Government would potentially incur as they relate to the proposed solutions for this contract. Any significant risk to the Government resulting from the sensitivity analysis may be reflected in the value proposition assessment. Cost/price risk refers to any aspect of an Offeror's proposal that may have significant negative cost consequences for FirstNet. Where risk is assessed, it may be described in qualitative terms and/or used as a best-value discriminator. The Government reserves the right to limit these detailed assessments to proposals that have been evaluated as technically acceptable in Phases II and III of this multi-phased approach. Additionally, the Government reserves the right to make any adjustment in costs, for evaluation purposes, in order to assess the overall cost to the Government depending on the outcome of the sensitivity analysis based on the proposed solution.

M.4.6 Risk

Each proposal will be assessed to identify potential risk. Risk refers to any aspect of an Offeror's proposal that could have significant negative consequences for the Government. Where risk is assessed, it may be described in qualitative terms and/or used as a best-value discriminator.

Additionally, the Government will assess the relative risks associated with each Offeror's proposal. It is important to note the distinction between proposal risk and performance risk.

- ***Proposal risks*** are those associated with an Offeror's proposed approach in meeting the objectives. Proposal risk is assessed by the proposal evaluators and is integrated into the rating of each specific evaluation factor in the overall evaluation.
- ***Performance risks*** are those associated with an Offeror's likelihood of success in performing the RFP's objectives as indicated by the Offeror's record of past performance. Performance risk is assessed by the proposal evaluators and is assigned a narrative rating in the performance risk (past performance) factor of the evaluation. Additionally, performance risk may be assessed and considered in the rating of each specific evaluation factor in the overall evaluation. The Government may conduct a performance risk assessment based upon the quality of the Offeror's past performance as well as that of its proposed subcontractors (if any), as it relates to the probability of successful accomplishment of the required effort. When assessing performance risk, the Government will focus its inquiry on the past performance of the Offeror and its proposed subcontractors as it relates to all RFP objectives, such as cost, schedule, and

performance, including the Offeror's record of containing and forecasting costs on any previously performed contracts; the Offeror's adherence to contract schedules, including the administrative aspects of performance; the Offeror's history for reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the Offeror's business-like concern for the interests of its customers.

A significant achievement, problem, or lack of relevant data in any element of the work may become an important consideration in the source selection decision. A negative finding under any element may result in an overall high-performance risk rating. Therefore, Offerors are reminded to include all relevant past efforts, including demonstrated corrective actions, in their proposal.

The Offeror's responsibility for award, as defined in FAR 9.104-1, including any special responsibility criteria identified herein will be considered.

M.5 Competitive Range

In accordance with FAR 15.306(c), after evaluating all proposals, if it has been determined to be in the best interest of the Government to establish a competitive range, the Government reserves the right to limit the competitive range for purposes of efficiency. The Government may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated technical proposals (10 U.S.C. 2305(b)(4) and 41 U.S.C. 253b(d)).

The competitive range will be comprised of the most highly rated technical proposals and those Offerors whose proposals have a reasonable chance of being selected for award. The competitive range determination is a qualitative judgment based on the factual content contained in the technical volumes.

Offerors are reminded that if the Contracting Officer determines that the number of proposals that would otherwise be in the competitive range exceeds the number at which an efficient competition can be conducted, the Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals. The Contracting Officer will promptly notify Offerors of any decision to exclude them from the competitive range.

M.6 Evaluation Support

The Government intends to use unbiased and conflict-free outside contractors to assist in the evaluation of proposals. These contractors will have access to any and all information contained in the Offeror's proposal and may participate in oral presentations and/or technical demonstrations if conducted, and will be subject to appropriate conflict of interest, standards of conduct, and confidentiality restrictions.