

Table of Contents

1	Purpose	1
2	FirstNet Overview and Mission	1
3	State Consultation	1
3.1	State Governing Body	1
3.2	[State Name] Consultation Process	1
3.3	Outreach and Education Support	1
3.4	State Plan Inputs and Outcomes.....	1
3.4.1	Minimum Criteria for a State Plan	1
3.4.2	Coverage Objectives	1
3.4.3	User Profiles/Statistics.....	1
3.4.4	Capacity Planning.....	1
3.4.5	Current Mobile Data Usage	1
3.5	State Decision Process	2
3.5.1	Summary/Timeline of Actions Required by the State	2
3.5.2	Changes to State Plan Following Decision to Proceed with FirstNet-Deployed Radio Access Network	2
4	State Radio Access Network Plan	2
4.1	Radio Access Network Partner	2
4.2	Network Design and Key Assumptions	2
4.2.1	Coverage Objectives and Requirements.....	3
4.2.2	RESERVED.....	3
4.2.3	Link Budget Specifications	3
4.2.4	Equipment Performance Specifications.....	3
4.2.5	Early Builder Integration	4
4.2.6	Temporary Coverage Related to Incidents and Planned Events	4
4.3	State Coverage Summary.....	4
4.3.1	Persistent Coverage	4
4.3.2	Coverage Extension Assets for Purchase by Public Safety Entities.....	5
4.3.3	Non-Persistent Cellular Service and Devices	5
4.4	Deployment Phases and Timelines	5
4.5	Rural Milestones	5
4.6	Network Upgrade and Expansion	6
4.7	State Assets.....	6
4.7.1	Memorandum of Understanding/ Memorandum of Agreement Requirements ..	6
4.7.2	Tower Sites.....	6
4.7.3	Backhaul.....	6
4.7.4	Other State Assets	6
4.8	Spectrum Clearing.....	6
5	Public Safety Grade	6
5.1	Coverage and Hardening	7
5.2	Installation	7

5.3	Operations and Maintenance	7
5.3.1	Service Availability	7
5.3.2	Customer Care and Support	8
5.3.3	Services Management Center.....	8
5.3.4	Status Reporting to States and Territories	9
5.3.5	Public Safety Enterprise Network/Public Safety Answering Point Integration	9
5.4	Network Reliability.....	10
5.5	Network Resiliency	10
5.6	Network Redundancy	10
5.7	Environmental Factors.....	10
5.8	Security	10
5.8.1	Security Architecture Plan	10
5.8.2	Security Integration and Test Plan.....	11
5.8.3	Applications Security Plan.....	11
5.8.4	Security Monitoring Plan	11
5.8.5	Security Configuration Management Plan.....	11
5.8.6	Technical Analysis and Security Review of Security Tools	11
5.8.7	Physical Security Plan.....	11
5.8.8	Cybersecurity Incident Response Plan.....	12
6	Network Operator/User Training Requirements	12
7	State Decision Process/Requirements/Timeline.....	12
7.1	Proceeding with FirstNet-Deployed RAN – Next Steps and Process to Submit Questions	12
7.2	Consultation Roles and Responsibilities after the Plan is Accepted.....	12
7.3	Decision to Proceed with State-Deployed RAN – Procedures	12
7.3.1	Decision to Proceed with State-Deployed RAN Plan Requirements.....	12
7.3.2	Decision to Proceed with State-Deployed RAN Plan Criteria	12
7.3.3	Decision to Proceed with State-Deployed RAN Plan Submission Process.....	12
7.4	Timeline	12
APPENDIX A	FirstNet Nationwide Design	13
A.1	End-to-End Network Architecture	13
A.1.1	State RAN Architecture	13
A.1.2	Nationwide Core Architecture	14
A.1.3	Backhaul, Aggregation, Transport, and National Transmission Network Architecture	14
A.1.4	Operational Support System Architecture	14
A.1.5	Business Support System Architecture	15
A.1.6	Applications Architecture	15
A.1.7	Interconnection Architecture	15
A.2	End-to-End Network Design (Logical and Physical)	16
A.2.1	Radio Access Network Design.....	16
A.2.2	Core Design.....	17
A.2.3	Backhaul and Transport Design	17
A.2.4	Operational Support System Design.....	18
A.2.5	Business Support System Design	18

	A.2.6	Applications and Services Design.....	19
	A.2.7	Interconnection Design.....	19
A.3		Products and Services.....	19
	A.3.1	Products Roadmap.....	20
	A.3.2	Services Roadmap.....	20
A.4		Nationwide Core Network.....	20
	A.4.1	Roaming Strategy.....	20
	A.4.2	Roaming Partner Integration.....	20
	A.4.3	Network Specifications.....	20
	A.4.4	Session Continuity.....	21
A.5		Logical Architecture (System Views for User and Control Plane).....	21
	A.5.1	Covered Leasing Agreement User Integration.....	21
	A.5.2	Compliance to 3GPP Standards MVNO Strategy.....	21
	A.5.3	Key Core Network Locations.....	22
	A.5.4	Radio Access Network Backhaul Architecture and Topology.....	22
	A.5.5	Radio Access Network Backhaul Aggregation Transport Network.....	22
	A.5.6	National Transmission Network.....	23
	A.5.7	Transport Security.....	23
	A.5.8	Routing and DRA strategy.....	24
	A.5.9	Transport Service Prioritization.....	24
A.6		Network Services.....	24
	A.6.1	Basic Services.....	25
	A.6.2	Mission Critical Services.....	26
	A.6.3	Quality of Service, Priority, and Preemption.....	26
A.7		Network Implementation.....	26
	A.7.1	Integration Partners.....	26
	A.7.2	Network Naming and Identification.....	26
	A.7.3	Design Assumptions.....	27
	A.7.4	IP Strategy.....	27
	A.7.5	Heterogeneous Network Integration.....	28
	A.7.6	Numbering Plan.....	28
	A.7.7	PSEN and PSAP Integration.....	28
	A.7.8	PSTN, ISP and Peering Integration.....	28
	A.7.9	PLMN and Roaming Partner Integration.....	29
	A.7.10	State-Deployed RAN Integration.....	29
	A.7.11	Support for LMR Network Integration.....	30
A.8		Project Plan/Schedule.....	30
	A.8.1	MVNO to NPSBN Core/RAN Migration.....	30
	A.8.2	Number Portability.....	31
APPENDIX B		Device Strategy, Roadmap, and Support.....	32
	B.1	Device Portfolio Available to PSE.....	32
	B.2	Device Acceptance Process.....	32
	B.3	Users.....	32
	B.4	Bring Your Own Device Policy.....	32
	B.5	Device Pricing.....	32
	B.6	Device Support and Life-Cycle Management.....	32

B.7	Local Control and Management of User Devices.....	32
B.8	Device Support of Network Services	33
B.9	Device Support of Commercial Band Access to Cellular Service	33
B.10	Roadmap for Device Support of New Features and Services	33
B.11	SIM/UICC Distribution Process and Management.....	33
APPENDIX C	Application Strategy and Operations	34
C.1	Baseline Launch Applications.....	34
C.2	Applications Storefront.....	35
C.3	Applications Management.....	35
C.4	Applications Security	35
C.5	Local Control	35
C.6	Applications Certification.....	35
C.7	Public Safety Entity Home Page	35
C.8	Applications Developer and Publication	36
C.9	API Taxonomy	36
C.10	Applications Product Roadmap	36
APPENDIX D	Deployable Assets	37
D.1	Deployable Operations	37
D.2	Fleet Management.....	37
D.3	Activation	37
D.4	Incident Management	37
D.5	Deployable Integration/Backhaul	37
D.6	Roles and Responsibilities (State or Territory/FirstNet)	37
APPENDIX E	Financials	38
E.1	Covered Leasing Agreement/Excess Network Capacity Value	38
E.2	FirstNet Value Proposition.....	38
E.3	User Fees/Costs	38
E.4	Procurement Vehicles.....	38
E.5	Funding Allocation for Buildout within the State or Territory.....	38
E.6	Core Network User Fee.....	38
E.7	Infrastructure Leasing Fee	38

List of Tables

Table 1	Map Deliverables for Coverage and Capacity	4
Table 2	Network Statistics Deliverables.....	5

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 restoration 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 NPSBN 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, PSEs, 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 perspective 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.