

Table of Contents

L	Instructions, Conditions, and Notices to Offerors or Respondents.....	L-1
L.1	FAR 52.252-1, Solicitation Provisions Incorporated by Reference (FEB 1998).....	L-1
L.1.1	FAR 52.216-1, Type of Contract (APR 1984)	L-1
L.1.2	FAR 52.252-5, Authorized Deviations in Provisions (APR 1984).....	L-1
L.1.3	FAR 52.233-2, Service of Protest (SEP 2006)	L-2
L.1.4	Independent Review of Protests to the Agency	L-2
L.1.5	Inquiries	L-2
L.1.6	Incurring Costs	L-2
L.1.7	Involvement of Current and Former Government Employees.....	L-3
L.1.8	Freedom of Information Act and Congressional Request	L-3
L.1.9	AQD Evaluation of Options Provision (OCT 2015)	L-3
L.1.10	1452.215-71, Use and Disclosure of Proposal Information (APR 1984)	L-4
L.2	General Instructions.....	L-5
L.2.1	Partnering/Teaming List	L-5
L.2.2	Pre-Proposal Conference	L-6
L.2.3	Formal Communication – Requests for RFP Clarification	L-7
L.2.4	Submission of Capability Statements	L-7
L.2.5	Submission of Proposals	L-9
L.2.6	Assumptions, Conditions, and/or Exceptions.....	L-10
L.3	Proposal Format and Submission Instructions	L-10
L.3.1	Volume I – Business Management.....	L-11
L.3.2	Volume II – Technical.....	L-18
L.3.3	Volume III – Pricing	L-57

List of Tables

Table 1	Solicitation Provisions Incorporated by Reference	L-1
Table 2	Coverage Maps Required for Coverage and Capacity.....	L-20
Table 3	Network Statistics Required for Coverage and Capacity	L-20
Table 4	Coverage Maps Required for Coverage and Capacity.....	L-28
Table 5	Network Statistics Required for Coverage and Capacity	L-28

List of Figures

Figure 1	Notional Contracting Process – Initial Years of IDIQ Contract.....	L-59.3
Figure 2	Notional Contracting Process – Final Years of IDIQ Contract	L-59.3

L Instructions, Conditions, and Notices to Offerors or Respondents

L.1 FAR 52.252-1, Solicitation Provisions Incorporated by Reference (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer (CO) will make their full text available. The Offeror is cautioned that the listed provisions may include blocks that must be completed by the Offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the Offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this address: <https://www.acquisition.gov/?q=browsefar>.

Table 1 Solicitation Provisions Incorporated by Reference

Clause Number	Title	Date
52.204-6	Data Universal Numbering System (DUNS) Number	JUL 2013
52.204-7	System for Award Management	JUL 2013
52.214-34	Submission of Offers in the English Language	APR 1991
52.214-35	Submission of Offers in U.S. Currency	APR 1991
52.215-1	Instructions to Offerors – Competitive Acquisition	JAN 2004
52.216-29	Time-and-Materials/Labor-Hour Proposal Requirements – Non-Commercial Item Acquisition With Adequate Price Competition	FEB 2007
52.222-24	Preaward On-Site Equal Opportunity Compliance Evaluation	FEB 1999
52.222-46	Evaluation of Compensation for Professional Employees	FEB 1993
52.237-10	Identification of Uncompensated Overtime	MAR 2015

L.1.1 FAR 52.216-1, Type of Contract (APR 1984)

The anticipated contract resulting from the Request for Proposal (RFP) will be a single award Indefinite-Delivery-Indefinite-Quantity (IDIQ) with fixed price payments to the First Responder Network Authority (FirstNet) by the Contractor for each of the 56 states and territories resulting from this solicitation.

(End of Clause)

L.1.2 FAR 52.252-5, Authorized Deviations in Provisions (APR 1984)

The use in this solicitation of any Federal Acquisition Regulation (48 Code of Federal Regulations [CFR] Chapter 1) provision with an authorized deviation is indicated by the addition of “(DEVIATION)” after the date of the provision.

The use in this solicitation of any Department of the Interior (DOI) Acquisition Regulation (48 CFR Chapter 14) provision with an authorized deviation is indicated by the addition of “(DEVIATION)” after the name of the regulation.

(End of Clause)

L.1.3 FAR 52.233-2, Service of Protest (SEP 2006)

Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the CO at the address below. A written, dated acknowledgement of receipt must be obtained. Address if mailed and/or hand carried:

Mr. Gregory Ruderman
U.S. Department of the Interior
Office of the Secretary, Interior Business Center
Acquisition Services Directorate
381 Elden Street, 4th Floor
Herndon, VA 20170

A copy of the protest served on the CO shall be simultaneously furnished by the protester to the Assistant Solicitor for Procurement and Patents, Office of the Solicitor, U.S. Department of the Interior, Room 6511, 1849 C Street, NW, Washington, DC 20240.

(End of Clause)

L.1.4 Independent Review of Protests to the Agency

Interested parties may request an independent review at a level above the CO of protests filed directly to the agency in accordance with Federal Acquisition Regulation (FAR) Part 33. This review is available as an alternative to consideration of the protest by the CO. Requests for independent review shall be submitted to the Chief of the acquisition office issuing the RFP, who will designate the official(s) to conduct the independent review.

L.1.5 Inquiries

Offerors are instructed to contact only the CO shown in Block 8 of Section A, Solicitation, Offer, and Award, for information about any aspect of this RFP. Prospective Offerors are cautioned against contacting government technical personnel in regard to this RFP prior to award of this procurement. If such a contact occurs and is found to be prejudicial to competing Offerors, the Offeror making such a contact may be excluded from further consideration for award.

Accordingly, all communications prior to award shall be directed to the CO named in Block 8 of Section A, Solicitation, Offer, and Award. Where possible, inquiries shall be submitted in writing, email, or as otherwise instructed herein. Questions should be worded so as to avoid disclosing any potential proposed strategies or proprietary solutions. Questions and answers will be provided to all Offerors being solicited via the Federal Business Opportunities site (www.fbo.gov).

L.1.6 Incurring Costs

The CO is the only person who can legally obligate the Government for the expenditure of public funds. Costs shall not be incurred by recipients of this RFP in anticipation of receiving direct reimbursement from the Government. It is understood that your proposal will become part of the official file on this matter without obligation of the Government.

L.1.7 Involvement of Current and Former Government Employees

Awards to current Government employees or firms owned or controlled by them are restricted by FAR 3.601 to exceptional cases approved by the head of the contracting activity. Restrictions regarding current employees apply to regular employees and special Government employees (such as the FirstNet Board) as those terms are defined in 43 CFR Section 20.735-1, Definitions. To avoid an appearance of impropriety, preferential treatment, or unfair competitive advantage, the Government has established additional disclosure and review requirements for awards to or involving former Government employees.

The prospective Contractor shall provide a disclosure statement in its proposal identifying any current Government employees or former Government employees who will be involved in the proposal and/or resultant contract and the nature of their involvement or financial interests if:

- The Offeror is a current or a former Government employee.
- The Offeror is a business concern substantially owned or controlled by one or more current or former Government employees.
- The Offeror has employed in the preparation of this proposal or plans to employ on any contract resulting from this RFP a current or a former Government employee.

Disclosure requirements regarding former employees are limited to former regular and special Government employees whose employment terminated within two years prior to submission of this RFP. Involvement of such employees, either in preparing the proposal or under any resultant contract, is not necessarily precluded, but each case shall be reviewed against standards of conduct and procurement integrity restrictions on former employees.

L.1.8 Freedom of Information Act and Congressional Request

Offerors are apprised that information furnished under this RFP may not be subject to disclosure under the Freedom of Information Act (FOIA), under Section 821 of P.L. No. 104-201 (1997) in accordance with the Act.

Offerors should nevertheless be aware that proposals may be accessed through congressional request and are advised to clearly mark all items that are confidential to the business or contain trade secrets, proprietary information, or personal information. Marking of items will not necessarily preclude mandatory disclosure.

L.1.9 AQD Evaluation of Options Provision (OCT 2015)

The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic award. This solicitation notified Offerors that the award will include the Government's unilateral option to extend performance for an additional period up to six months under FAR 52.217-8, during which the pricing and terms of the period in which the option was exercised would apply. The Government cannot predict if or when the option may be exercised. Because any exercise of the Government's option extends the pricing and terms of the period in which the option was exercised, the Government expressly and affirmatively evaluates pricing for the option to extend under 52.217-8 co-extensive with the Government's price evaluation for each of the base and option periods of this award. Because pricing for each period subject to possible extension under the 52.217-8 has been evaluated, pricing for any possible future use of that option to extend has, likewise, been evaluated and would apply in strict accordance with this evaluation in the event of the Government's exercise of the option to extend services.

(End of Provision)

L.1.10 1452.215-71, Use and Disclosure of Proposal Information (APR 1984)

(a) Definitions. For the purposes of this provision and the Freedom of Information Act (5 U.S.C. 552), the following terms shall have the meaning set forth below:

(1) “Trade Secret” means an unpatented, secret, commercially valuable plan, appliance, formula, or process, which is used for making, preparing, compounding, treating or processing articles or materials which are trade commodities.

(2) “Confidential commercial or financial information” means any business information (other than trade secrets) which is exempt from the mandatory disclosure requirement of the Freedom of Information Act, 5 U.S.C. 552. Exemptions from mandatory disclosure which may be applicable to business information contained in proposals include exemption (4), which covers “commercial and financial information obtained from a person and privileged or confidential,” and exemption (9), which covers “geological and geophysical information, including maps, concerning wells.”

(b) If the Offeror, or its subcontractor(s), believes that the proposal contains trade secrets or confidential commercial or financial information exempt from disclosure under the Freedom of Information Act, (5 U.S.C. 552), the cover page of each copy of the proposal shall be marked with the following legend:

“The information specifically identified on pages [to be completed by the Contractor] of this proposal constitutes trade secrets or confidential commercial and financial information which the Offeror believes to be exempt from disclosure under the Freedom of Information Act. The Offeror requests that this information not be disclosed to the public, except as may be required by law. The Offeror also requests that this information not be used in whole or part by the government for any purpose other than to evaluate the proposal, except that if a contract is awarded to the Offeror as a result of or in connection with the submission of the proposal, the Government shall have the right to use the information to the extent provided in the contract.”

(c) The Offeror shall also specifically identify trade secret information and confidential commercial and financial information on the pages of the proposal on which it appears and shall mark each such page with the following legend:

“This page contains trade secrets or confidential commercial and financial information which the Offeror believes to be exempt from disclosure under the Freedom of Information Act and which is subject to the legend contained on the cover page of this proposal.”

(d) Information in a proposal identified by an Offeror as trade secret information or confidential commercial and financial information shall be used by the Government only for the purpose of evaluating the proposal, except that (i) if a contract is awarded to the Offeror as a result of or in connection with submission of the proposal, the Government shall have the right to use the information as provided in the contract, and (ii) if the same information is obtained from another source without restriction it may be used without restriction.

(e) If a request under the Freedom of Information Act seeks access to information in a proposal identified as trade secret information or confidential commercial and financial information, full consideration will be given to the Offeror's view that the information constitutes trade secrets or confidential commercial or financial information. The Offeror will also be promptly notified of the

request and given an opportunity to provide additional evidence and argument in support of its position, unless administratively unfeasible to do so. If it is determined that information claimed by the Offeror to be trade secret information or confidential commercial or financial information is not exempt from disclosure under the Freedom of Information Act, the Offeror will be notified of this determination prior to disclosure of the information.

(f) The Government assumes no liability for the disclosure or use of information contained in a proposal if not marked in accordance with paragraphs (b) and (c) of this provision. If a request under the Freedom of Information Act is made for information in a proposal not marked in accordance with paragraphs (b) and (c) of this provision, the Offeror concerned shall be promptly notified of the request and given an opportunity to provide its position to the Government. However, failure of an Offeror to mark information contained in a proposal as trade secret information or confidential commercial or financial information will be treated by the Government as evidence that the information is not exempt from disclosure under the Freedom of Information Act, absent a showing that the failure to mark was due to unusual or extenuating circumstances, such as a showing that the Offeror had intended to mark, but that markings were omitted from the Offeror's proposal due to clerical error.

(End of provision)

L.2 General Instructions

Your proposal shall become the property of the Government and will not be returned. If your proposal contains information that you do not wish disclosed to the public or used by FirstNet for any purpose other than evaluation of your proposal, such restrictions shall be clearly indicated on each sheet containing such information (see FAR 52.215-1 listed in Table 1 Solicitation Provisions Incorporated by Reference).

Prior to submission of a proposal, the Offeror is expected to reach an understanding of the objectives of this RFP. If such a review establishes the need for correction or clarification, such information should immediately be brought to the attention of the CO, in accordance with the instructions contained herein, so that the matter can be resolved and, if necessary, official dissemination of such information can be made to all Offerors.

The Government reserves the right to request additional information as may be necessary to determine the Offeror's qualifications for award or to clarify any aspects of the Offeror's proposal. Such information shall be furnished promptly upon the Government's request.

Offerors shall not be reimbursed for the costs of developing a proposal for this RFP.

One copy of each unsuccessful proposal will be retained in the contract file and all other copies will be destroyed. Additional copies of the successful proposal may be retained only as needed for contract administration and monitoring.

L.2.1 Partnering/Teaming List

As a courtesy, the Government has been compiling a list of those Offerors interested in subcontracting and teaming opportunities with other potential Offerors. If you are interested in being included on the list, please submit your business name and size and point of contact information (e.g., name, email address, phone number) no later than **2:00 p.m. Eastern Time on Thursday, March 17, 2016**, to the

point of contact identified herein. All email inquiries shall have “Teaming List – RFP # D15PS00295” included in the subject line.

The partnering/teaming list is available via the Federal Business Opportunities (FBO) website (www.fbo.gov) and the FirstNet website (www.FirstNet.gov). Offerors are not required to be listed on the partnering/teaming list to submit a proposal. This is optional and solely intended to be a list of potential subcontracting and teaming opportunities. This list of potential subcontractors/teaming partners is not evaluated by the Government and, therefore, the Government accepts no liability for any resultant outcomes. Being placed on the list does not obligate the Government or any other party to make an award, subcontract award, or any other business opportunity.

L.2.2 Pre-Proposal Conference

The Government anticipates holding a pre-proposal conference and highly encourages Offerors to attend (in person or via webcast). However, attendance is not a prerequisite for submitting a proposal. The purpose of the pre-proposal conference is to provide potential Offerors the opportunity to further understand FirstNet’s approach to the Nationwide Public Safety Broadband Network (NPSBN) and to ask questions, time permitting. At the Government’s discretion, the Government will respond to RFP questions either verbally at the conference or in writing following the conference.

L.2.2.1 Pre-Proposal Conference Date, Time, and Location

Date	March 10, 2016
Time	From 1:30–5:00 p.m. Eastern Time
Registration Time	1:00 p.m. Eastern Time
Location	U.S. Geological Survey National Center Auditorium 12201 Sunrise Valley Drive Reston, VA 20192

L.2.2.2 Pre-Proposal Conference Attendance

Offerors may participate in the pre-proposal conference in person or remotely via webcast. Both the on-site event and the webcast will be free and open.

Pre-registration is required for on-site attendance as space may be limited. To pre-register, attendees shall send an email to FirstNetIndustryDay@firstnet.gov. On-site attendance is limited to three individuals from each company or organization. Registration is not required for the webcast.

On-site attendance will be on a first-come, first-served basis during pre-registration. Once the maximum number of attendees is reached, registration will close and subsequent requests for on-site participation will be denied. On March 10, 2016, pre-registered attendees will be required to check in on-site. Check-in will commence at 1:00 p.m. Eastern Time. Those who have not pre-registered will not be admitted.

In the event of any time and/or date changes to the pre-proposal conference, the Government will notify Offerors via an amendment to the RFP posted to FBO (www.fbo.gov).

L.2.2.3 Pre-Proposal Conference Questions and Answers

Offerors may ask questions at the pre-proposal conference or provide those questions in writing (via email) to the Government prior to the pre-proposal conference. These questions shall be submitted in

accordance with the instructions stated in Section L.2.3, Formal Communication – Requests for RFP Clarification.

The Government will only accept questions submitted by email utilizing the Questions Template in Section J, Attachment J-5; questions submitted by any other means, such as voicemail or fax will not be accepted. The Government will not attribute questions to the authors. This RFP may be amended as a result of the Government's response, and any amendments will govern over the posted questions/responses.

L.2.3 Formal Communication – Requests for RFP Clarification

The opportunity to submit all requests for RFP clarification begins upon the release of the RFP and ends no later than **1:00 p.m. Eastern Time on Friday, February 12, 2016**. All requests for clarification shall be submitted in writing by email, as identified in Section J, Attachment J-5, Questions Template. The Offeror shall send requests for clarification to FirstNetRFPQuestions@firstnet.gov. All submissions shall reference this RFP number and title.

Requests transmitted via fax or phone will not be accepted.

Should any request for clarification be received after the date and time stated above, the Government reserves the right not to provide an answer. If, however, the Government determines the request for clarification addresses an issue of significant importance, the Government may provide a written response to all Offerors. Please note, questions and/or comments will not be protected by the Government as proprietary (see Section L.1.5, Inquiries).

Additionally, Offerors may determine or believe that the RFP package contains errors or omissions, or is otherwise unsound. In such cases, the Offeror shall immediately notify the CO in writing of such errors, omissions, or other issues in accordance with the instructions regarding submission of questions. The Offeror shall provide details and supporting rationale.

L.2.4 Submission of Capability Statements

As stated in Section M, Evaluation Factors for Award, Phase I of the multi-phased approach is submission of capability statements (see FAR Part 15.202). Interested parties should demonstrate they are qualified to perform the work by providing their capabilities as stated herein. The capability statement shall not exceed 50 pages in length (25 sheets of paper, double-sided print, 8.5" x 11" size paper) and shall be provided in Adobe PDF or Microsoft Word soft copy file format with Times New Roman font of 12 points or higher. Tables, charts, figures, and headers and footers may use a font size other than point 12 as long as it is legible. Any pages that exceed the 50-page limit will not be evaluated. The capability statement should provide information detailing:

- **Public safety use and adoption of the NPSBN** – Information demonstrating the Offeror's ability to successfully drive adoption and use of the NPSBN by public safety users.
- **Nationwide coverage and capacity** – Information demonstrating the Offeror's ability to provide Band 14 and non-Band 14 coverage and capacity in each of the 56 states and territories, including rural and non-rural areas.
- **Rural partnerships** – Information demonstrating the Offeror's existing and planned partnerships with rural telecommunications providers, including commercial mobile providers, utilizing existing infrastructure to the maximum extent economically desirable to speed deployment in rural areas.

- **Ability to monetize network capacity** – Information demonstrating the Offeror’s strategy and demonstrating its ability to monetize network capacity, which may include a secondary user customer base and sales/distribution channels to reach primary and secondary users.
- **Financial sustainability** – Information demonstrating the Offeror’s approach and financial sustainability. Additionally, information demonstrating its ability to develop, implement, sustain, and enhance the NPSBN based on the Initial Operational Capability (IOC)/Final Operational Capability (FOC) milestones set out in Section J, Attachment J-8, IOC/FOC Target Timeline.

The capability statement shall be received on or before **2:00 p.m. Eastern Time on Thursday, March 31, 2016**. The capability statement shall be submitted in hard copy (one original and eight hard copies) and on three flash drives in Adobe PDF or Microsoft Word soft copy file format (to be submitted with the hard copies) to the addresses stated herein. In the event the hard copy and soft copy content conflict, the hard copy submission will take precedence over the soft copy version.

Please note it is the Offeror’s responsibility to ensure/verify that the Government receives its submission on or before the date and time specified. If the capability statement is not received by the Government on or before the date and time specified, the Offeror’s submission may be considered late.

The addresses designated for receipt of capability statements is:

ORIGINAL AND SEVEN (7) HARD COPIES AND TWO FLASH DRIVES TO:

Ms. Terrie L. Callahan
U.S. Department of the Interior
Office of the Secretary, Interior Business Center
Acquisition Services Directorate
381 Elden Street, 4th Floor
Herndon, VA 20170
Phone: 703-964-3596

ONE (1) HARD COPY AND ONE FLASH DRIVE TO:

Primary Points of Contact: Ms. Peggy O’Connor and Mr. Mouncef Belcaid
Alternate Point of Contact: Mr. Jordan Andrews and Mr. Michael Carroll
First Responder Network Authority
3122 Sterling Cir, Suite 100
Boulder, CO 80301

Phone: (303) 334-9660
Alternate Phone: (303) 334-9661

Please note that DOI locations are secured buildings. If offers are hand delivered, instruct the courier to check in at the guard desk and ask to call the point of contact identified above. A staff member will meet the courier to receive the submittal. All packages containing a capability statement shall be labeled and sealed as if for mailing, and the following information shall be marked on the outside:

- Capability statement for RFP number
- Date and time specified for receipt
- Name and address of the Offeror

- Name of the DOI/Interior Business Center (IBC) point of contact (Ms. Terrie L. Callahan in Herndon, VA) or the FirstNet points of contact (Ms. Peggy O'Connor and Mr. Mouncef Belcaid in Boulder, CO)

When submissions are hand carried or delivered by courier service or express delivery service (e.g., Federal Express, DHL), the Offeror assumes full responsibility for ensuring allocation of enough time to gain access to the IBC, Acquisition Services Directorate (AQD) staff in accordance with these instructions and to submit its capability statement by the time and date specified herein.

As stated above, please be advised that it is the Offeror's responsibility to ensure the Government receives its submission on or before the specified due date and time.

L.2.5 Submission of Proposals

Proposals shall be received ***on or before 2:00 p.m. Eastern Time on Tuesday, May 31, 2016***. Proposals shall be submitted in hard copy (one original and eighteen hard copies) and on two flash drives in Adobe PDF or Microsoft Word soft copy file format, with the exception of any Excel, map, and shape files, to be submitted with the hard copies. In the event the hard copy and soft copy content conflict, the hard copy version will take precedence over the soft copy version.

Please note it is the Offeror's responsibility to ensure/verify that the Government receives its submission on or before the date and time specified. If the proposal is not received by the Government on or before the date and time specified, the Offeror's submission may be considered late. Timeliness of receipt of any submission will be determined by the date and time received at the Reston, VA address shown herein.

The addresses designated for receipt of proposals is:

ORIGINAL AND THIRTEEN (13) HARD COPIES AND ONE FLASH DRIVE TO:

Mr. Gregory Ruderman (Department of the Interior, Acquisition Services Directorate)
U.S. Department of Commerce
First Responder Network Authority
12200 Sunrise Valley Drive, Suite 100
Reston, VA 20191-3402

Office Phone: (703) 964-3590

FIVE (5) HARD COPIES AND ONE FLASH DRIVE TO:

Primary Points of Contact: Ms. Peggy O'Connor and Mr. Mouncef Belcaid
Alternate Points of Contact: Mr. Jordan Andrews and Mr. Michael Carroll
First Responder Network Authority
3122 Sterling Cir, Suite 100
Boulder, CO 80301

Phone: (303) 334-9660
Alternate Phone: (303) 334-9661

Please note that these locations are secured buildings. If offers are hand delivered, instruct the courier to check in at the guard desk and ask to call the points of contact identified above. A staff member will meet the courier to receive the submittal. All packages containing proposal submissions shall be labeled and sealed as if for mailing, and the following information shall be marked on the outside:

- RFP number
- Date and time specified for receipt
- Name and address of the Offeror
- Name of the DOI/IBC point of contact (Mr. Gregory Ruderman in Reston, VA) or the FirstNet points of contact (Primary: Ms. Peggy O'Connor and Mr. Mouncef Belcaid or Alternate: Mr. Jordan Andrews and Mr. Michael Carroll in Boulder, CO)

When submissions are hand carried or delivered by courier service or express delivery service (e.g., Federal Express, DHL), the Offeror assumes full responsibility for ensuring allocation of enough time to gain access to the secure facility for submission delivery in accordance with these instructions and to submit its proposal by the time and date specified herein.

As stated above, please be advised that it is the Offeror's responsibility to ensure the Government receives its submission on or before the specified due date and time.

L.2.6 Assumptions, Conditions, and/or Exceptions

The Offerors shall submit, under a separate tab, *in each volume identified herein*, all (if any) assumptions, conditions, or exceptions with any of the terms and conditions of this RFP. If not noted in its proposal, it will be assumed that the Offeror proposes no assumptions, conditions, or exceptions for award and agrees to comply with all of the terms and conditions as set forth herein. It is not the responsibility of the Government to seek out and identify assumptions, conditions, or exceptions buried within the Offeror's proposal.

For proposal preparation purposes, if there are any assumptions, conditions, or exceptions made pertaining to demarcation between the Government's responsibility and/or the Contractor, the Offeror shall describe the specific demarcation points and/or assumptions, conditions, or exceptions within the proposal submission.

L.3 Proposal Format and Submission Instructions

Proposals, signed by an official authorized to bind the Offeror, shall set forth full, accurate, and complete information as required by this RFP. The penalty for making false statements is prescribed in 18 U.S.C. § 1001. Failure to furnish full and complete information requested may cause an offer to be determined unacceptable, and it may be removed from consideration for award.

In responding to this RFP, the Offerors shall prepare and submit the indicated numbers of copies (see Section L.2.5, Submission of Proposals) and required information that constitutes the Offeror's complete proposal submission. Additionally, the Offeror's information and submission shall be organized by volume as indicated below. Each volume shall include an Executive Summary that shall not exceed 4 pages in length (2 sheets of paper, double-sided print); each Executive Summary must clearly identify what portions of the volume are provided in soft-copy format (as allowed in accordance with Section L) for verification and validation purposes. Specifically, the business management volume shall be separate from the technical and pricing volumes.

Any page limitation for each proposal volume is identified within that section. However, the following information applies to *each* volume. The volumes shall be provided in Adobe PDF or Microsoft Word soft copy file format. A page is defined as Times New Roman Font Size 12, single-spaced, 8.5” x 11” (with the exception of the submission of maps and required Section J spreadsheets pertaining

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

to network statistics, which may use 11" x 17" size paper) with one (1) inch margins top, bottom, left, and right. Tables, charts, figures, and headers and footers may use a font size other than point 12 as long as it is legible. The page limitation excludes the cover page; Executive Summary; Section A, Solicitation, Offer, and Award; signed acknowledgements; table of contents and listing of tables, drawings, and/or exhibits; small business subcontracting plan; past performance references; and financial resources as identified herein. The Government shall treat page limitations as maximums. If exceeded, the CO will remove the excess pages prior to evaluation. The Government will not read or evaluate removed pages.

The Government reserves the right to request Offerors to conduct oral presentations and/or technical demonstrations as a result of this RFP (see Section M, Evaluation Factors for Award, Section M.2, Evaluation Process).

Proposal submittals to the Government shall be in three (3) volumes: Business Management, Technical, and Pricing.

L.3.1 Volume I – Business Management

The business management volume contains all information needed to communicate to the Government that the Offeror has well-developed processes in place to ensure effective program management and disciplined fiscal processes as identified within this section. Additionally, the Offeror shall include a small business subcontracting plan, Contractor responsibility information, and information on past performance in this volume.

The business management proposal shall not exceed 200 pages in length (100 sheets of paper, double-sided print). This page count excludes those items identified in Section L.3.1.1, Section One – General; the Solicitation Conformance Traceability Matrix; the Small Business Subcontracting Plan; Past Performance reference forms; the resumes, Integrated Master Schedule, and Work Breakdown Structure (WBS) referenced in L.3.1.2, Section Two – Leadership and Program Management; the Public Safety Device Connections Template and Section J, Attachment J-23, End User Pricing Tables, referenced in L.3.1.3, Section Three – Public Safety Customer Acquisition; Quality Assurance Surveillance Plan (QASP) reference in Section L.3.1.4, Section Four – Customer Care and Life-Cycle Sustainment; all items identified in Section L.3.1.5, Section Five – Offeror Financial Sustainability; and the executed Parental Guarantee Agreement identified in Section J, Attachment J-27. The business management proposal shall contain the following information and be broken down in the following sections.

L.3.1.1 Section One – General

The Offeror shall complete blocks 13, 15, 16, and 18 of Section A, Solicitation, Offer, and Award, and sign block 17 to show that the Offeror has read and agrees to comply with all the terms, conditions and instructions provided in the RFP unless otherwise noted in the assumptions, conditions, or exceptions section pertaining to the proposed solution. If there are any amendments to the RFP, the Offeror shall complete block 14 of Section A, Solicitation, Offer, and Award, and include a signed acknowledgement for all RFP amendments.

The Offeror shall describe its corporate management structure as well as the structure of the proposed team and the relationship between these organizations and all subcontractors proposed to perform all aspects of the objectives (as defined by the Offeror). Indicate the date the contracting entity was organized and indicate whether the organization is a separate entity, a division, or subsidiary

corporation. If it is a division or subsidiary corporation, provide the name and address of the parent company. Include your Taxpayer Identification Number (TIN) and DUNS number.

This volume shall also contain a section that includes a statement of intention to comply with the objectives stated herein and a statement of intention to comply with all terms and conditions of the contract unless otherwise noted in the assumptions, conditions, or exceptions section pertaining to the proposed solution.

As part of Volume I, Business Management, the Offeror shall propose a Performance Work Statement (PWS) identifying the tasks required for the deployment and operation of the NPSBN. The PWS shall address the objectives specified in Section C, Statement of Objectives (SOO) and the associated attachments in Section J. The PWS, evaluated to be the best overall solution, will replace the SOO in the subsequent contract.

Volume I, Business Management, shall also include separate tabs noting the solution for each Day 1 task order identified in Section B, Supplies or Services and Prices/Costs, Section B.2.1, Day 1 Task Orders. Each separate tab noting the solution for each Day 1 task order shall not exceed 50 pages in length (25 sheets of paper, double-sided print).

L.3.1.1.1 Solicitation Conformance Traceability Matrix

The Offeror shall fill out the Solicitation Conformance Traceability Matrix (SCTM)—available in Section J, Attachment J-22, SCTM—indicating the proposal reference information as it relates to the documents included in the RFP. If this matrix conflicts with any other requirement, direction, or provision of this RFP, the other reference and RFP information will take precedence over the Contractor-completed SCTM.

L.3.1.1.2 Small Business Subcontracting Plan Requirements

Offerors that qualify as large businesses shall submit a small business subcontracting plan following the guidelines identified in FAR 52.219-9, Small Business Subcontracting Plan (OCT 2015).

The plan submitted under this RFP shall comply with the format contained in Section J, Attachment J-26, Sample Small Business Subcontracting Plan.

The CO will make an affirmative determination regarding the acceptability of the small business subcontracting plan as one of the elements in determining eligibility for award.

Offerors that intend to use a subcontractor in performance of this contract shall provide evidence of the proposed subcontractor's commitment. If proposing a joint venture, the Offeror shall provide a copy of the joint venture plan/agreement. The Offeror shall describe how small business participation will contribute to its overall comprehensive subcontracting goals. The Offeror shall describe specific efforts to ensure the resulting contract meets or exceeds proposed small business subcontracting goals.

The requirements of clause FAR 52.219-9 and this provision do not apply when 1) the Offeror is a small business; 2) the work is to be performed entirely outside of any state, territory, or possession of the United States; the District of Columbia; and the Commonwealth of Puerto Rico; or 3) the contract, including all future modifications, will not exceed \$700,000. The requirement may also be waived if the CO determines that the resultant contract does not offer subcontracting opportunities.

L.3.1.1.3 Contractor Responsibility Information

The Offeror shall provide information demonstrating that it is responsible within the meaning of FAR 9.104-1. In addition to the general responsibility standards in FAR 9.104-1, there is a special

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

responsibility standard that applies to this solicitation. This standard applies to all Offerors. In order to be determined responsible on this solicitation, an Offeror shall demonstrate expertise needed for adequate contract performance. The Offeror shall present evidence that it (1) has experience in efficiently managing complex engineering, development, and operational activities; (2) has experience in rapidly designing, deploying, operating, and optimizing state-of-the-art communications networks; and (3) has ready access to and experience in attracting and retaining appropriate talent.

L.3.1.1.4 Past Performance

The Offeror shall provide three (3) references of same and/or similar efforts performed by the Offeror and/or any/all subcontractors and/or teaming partners within the last three years. Each reference shall include the following information:

- Project title
- Description of the project
- Contract number (if applicable)
- Government agency/non-Government organization
- Contracting Officer's Representative/contract point of contact's name, address, email address, and phone number
- CO/contract point of contact's name, address, email address, and phone number
- Current status, i.e., completed (start and end dates) or in progress (start and estimated completion dates)
- Dollar value and type of contract
- Key personnel (highlight those individuals who worked on the relevant project and are being proposed for this effort)

The Offeror shall detail existing 3rd Generation Partnership Program (3GPP) standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its subcontractors and/or teaming partners. This would include additional details of existing public safety networks and infrastructure operated, controlled, or managed by the Offeror or its partners.

Refer to Section J, Attachment J-25, Past Performance Reference Information Form, for a sample format. If you believe the Government may find derogatory information as a result of checking your past performance record, please provide an explanation and any remedial action taken by your organization to address the problem(s).

In the case where an Offeror does not have any relevant past performance and/or experience related to the objectives identified in Section C, SOO, it shall provide an explanation in the Past Performance section of the Business Management volume. The Government may also consider information obtained through other sources. For Offerors with no relevant past performance, the Government may take into account information regarding the past performance of personnel with relevant past performance or subcontractors that will perform key aspects of this contract.

The Past Performance section of the Business Management volume may address any other topics considered pertinent to a demonstration of the Offeror's knowledge, competence, and capability to perform this contract.

L.3.1.1.5 Offeror's Experience

Describe the Offeror's experience as it relates to the overall proposed solution for the NPSBN. This shall include the structure and experience of the proposed subcontractors/teaming partners, and the relationship between these organizations proposed to perform major or critical aspects of the NPSBN (as defined by the Offeror) shall be listed. If there are any items stated in Section L.3.1.1.4, Past Performance, that are also applicable to the Offeror's current experience, these shall be addressed in this section. Specifically, the Offeror shall detail current 3GPP standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its subcontractors and/or teaming partners. This would include additional details of existing public safety networks and infrastructure operated, controlled, or managed by the Offeror or its partners.

L.3.1.2 Section Two – Leadership and Program Management

To demonstrate its expertise in leadership and program management, the Offeror shall:

- Provide a management plan that describes the proposed approach to meet the objectives as defined in Section C, SOO, and associated attachments in Section J. This shall include but is not limited to a corporate-level organizational structure with charts to identify the size, scope, and structure of the Offeror's entity; a comprehensive program management approach reflecting the Offeror's ability to provide seamless and efficient management of the NPSBN for the life of the contract; a change management approach, including relevant processes and procedures; the proposed approach for managing the contract at the corporate, contract, and task order levels; the proposed approach for supporting and facilitating FirstNet's compliance with the Act and other applicable laws; and proposed escalation and resolution procedures, including planned integration and coordination with FirstNet personnel.
- Provide a staffing plan that includes but is not limited to the Offeror's proposed organizational structure for leadership of the NPSBN; identify staffing, including roles and responsibilities as well as resumes, for key personnel and executive leaders who will support FirstNet.
- Provide an Integrated Master Schedule and WBS that addresses all build-out and transition-to-operations activities. The Offeror shall note, in the WBS, those tasks that include deliverables. The Offeror shall identify, in the WBS, the tasks required for the deployment and the operation of the NPSBN such that the objectives (specified in Section C, SOO, and the associated attachments in Section J) are met at the task and subtask level. The Offeror shall propose a milestone timeline detailing its solution in accordance with the IOC/FOC milestones contained in Section J, Attachment J-8, IOC/FOC Target Timeline.
- Provide details of existing 3GPP standards-based mobile broadband service capabilities, mobile and fixed broadband infrastructure, and operations controlled or managed by the Offeror or its proposed teaming partners and/or subcontractors.
- Describe how the solution leverages existing commercial and/or other infrastructure.

L.3.1.3 Section Three – Public Safety Customer Acquisition

To demonstrate its ability to acquire and retain public safety customers, the Offeror shall, at a minimum:

- Complete the Public Safety Device Connections Template (Section J, Attachment J-24, PS Device Connections tab), detailing the Offeror's anticipated number of public safety device connections for the primary user group, which consists of law enforcement, fire, and emergency medical

services users, as well as the extended primary user group, which consists of all other public safety users, as defined in the Act. The number of connections shall be broken out by each of the 56 states and territories over the life of the IDIQ contract. For proposal planning and evaluation purposes, the Offeror shall assume that connection targets start from the

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

estimated task order date (as defined in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders). For example, year 1 of the Public Safety Device Connections Template (Section J, Attachment J-24, PS Device Connections tab) corresponds with the first year of the task order award. Actual state and territory task order awards will trigger the IOC/FOC milestones (Section J, Attachment J-8, IOC/FOC Target Timeline) and the disincentive mechanism as detailed in the QASP (Section J, Attachment J-6, Quality Assurance Surveillance Plan). Connections proposed by the Offeror, beyond the IDIQ period of performance, will not be subject to the disincentive mechanism detailed in the QASP (Section J, Attachment J-6, Quality Assurance Surveillance Plan).

- FirstNet has aggregated stakeholder data to produce a nationwide view that estimates the current subscriber and device demand at a state level for the primary user group, which consists of law enforcement, fire, and emergency medical services users, as well as the extended primary user group, which consists of all other public safety users, as defined in the Act. This information can be found in the Public Safety Device Connections Template (Section J, Attachment J-24) in the Users_Devices_By State worksheet and can be used as a reference by the Offeror when detailing the Offeror's anticipated number of public safety device connections. The estimates were developed based on input from states, territories, tribal nations, and federal agencies, as well as FirstNet estimates.
- Describe the Offeror's approach to sales and marketing to public safety within the context of its greater corporate strategy.
- Identify the go-to-market strategy and sales channels to be used by the marketing and sales organization(s) in offering, selling, and marketing services to public safety users. Channels may include but are not limited to direct, indirect, third party, Internet, telemarketing, and strategic alliances.
- Describe a strategy to collaborate with public safety stakeholders, associations, and other pertinent organizations, such as the Association of Public-Safety Communications Officials, National Association of State Chief Information Officers, International Association of Chiefs of Police, and Public Safety Advisory Committee.
- Describe public safety end-user pricing strategies for all products, services, and devices. These strategies shall include details on priority and preemption for public safety as well as public safety services for both post-paid and pre-paid service offerings on Band 14 and non-Band 14 networks. Complete the tables in Section J, Attachment J-23, End-User Pricing Tables, which represent indicative pricing and service plans available to public safety users. When completing the tables, include any assumptions, as instructed herein, used in determining indicative pricing—such as details on usage caps, roaming caps, throttling, and contract length—and describe any proposed volume discount schedule and special pricing mechanisms to support public safety adoption and use of the NPSBN.
- Describe the Customer Relationship Management (CRM) systems and tools that will be used in support of selling FirstNet devices and services and how the Offeror will report on related Key Performance Indicators (KPIs).
- Describe the form and functionality of a FirstNet-branded, customer-facing Web-based portal that will enable public safety users, including individually liable and enterprise-liable customers, to view and order, among others, devices, service offerings, and accessories.
- Describe the approach to foster a vibrant applications ecosystem. This shall include but is not limited to:
 - A strategy to market the FirstNet applications store and target public safety users

- A description and details of current or planned agreements and contracts with providers of software applications applicable to the public safety market
- Marketing strategies that will be implemented to attract and work with developers for public safety applications development
- Social media platforms to engage the public safety community
- Describe details of its sales and marketing structure, particularly sales and marketing channels specific to public safety, and if no channels specific to public safety, describe plans for developing or leveraging such channels. Describe the marketing and sales organization(s) tasked with supporting FirstNet, including but not limited to the organization's function, size, structure, geographic distribution (e.g., whether resources are based in the United States; the location and number of employees/subcontractors located outside of the United States), and relation to the Offeror (e.g., direct, indirect, outsourced). Additionally, describe the proposed approach to ensure strategic alignment and mitigation of sales and marketing channel conflict among teaming partners to ensure adoption and use of the NPSBN.
- Describe how the proposed solution will meet current, emerging, and future public safety needs, requirements, and standards. Explain how the services, devices, and applications ecosystems will evolve over the life of the contract; how the proposed services tie back to a network deployment plan; and when services will be generally available. Additionally, provide a roadmap of the existing and future Band 14 products, services, and devices to be offered and describe how new services and features will incentivize use of the NPSBN. Complete Table 3 in Section J, Attachment J-23, End-User Pricing Tables, to identify the anticipated supplier and estimated price points for Band 14-enabled devices for public safety.

L.3.1.4 Section Four – Customer Care and Life-Cycle Sustainment

The Offeror shall provide the following information regarding public safety service delivery, including all linkages to sales, marketing, fulfillment, customer care, and other relevant functions:

- Describe how the metrics proposed and outlined in the Offeror's proposed Quality Assurance Surveillance Plan (QASP) will be used to monitor and manage the service delivery system—including activation, repair, technical assistance, replacement devices, and emergency restoration—and customer satisfaction over the life of the contract.
- Describe the Offeror's proposed customer care strategy, which shall address:
 - How the Offeror will minimize churn and promote customer retention among public safety users.
 - How an integrated customer care model will be delivered for public safety users.
 - The customer care organization(s) that will support the NPSBN, including the organization's function, size, structure, geographic distribution (e.g., whether resources are based in the United States; the location and number of employees/subcontractors located outside of the United States), and relation to the Offeror (i.e., in-house, contracted out).
 - The proposed solution for resolving customer service requests or issues with service delivery or products.
 - How the Offeror will provide responsive corrective action for service impairments and service restoral when the action involves direct contact with the customer.
 - How the Offeror will train the customer on device or service usage.

- The proposed strategies for recruitment and retention of the customer care workforce, including how to train staff on existing and emerging products, services, and applications.
- Customer care systems and tools that will be used in support of public safety customer care.
- Detail the proposed comprehensive billing management strategy for public safety. The strategy shall include but is not limited to descriptions of the current billing support services for broadband services, wireless services, and, if applicable, public safety services; the billing support service delivery for the NPSBN; customized billing available for state, local, and tribal agencies using the NPSBN; and the Offeror's approach to billing throughout the FirstNet service area, including proposed roaming charges.

L.3.1.5 Section Five – Offeror Financial Sustainability

To allow the Government to assess if the Offeror has the financial sustainability to develop, implement, sustain, and enhance the NPSBN in accordance with the time frames, duration, and objectives set out in this RFP, the Offeror shall provide the financial information listed below. If the Offeror represents a consortium, partnership, or any other form of a joint venture, appropriate information shall be provided for all such entities comprising the Offeror.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

L.3.1.5.1 Financial Resources

The Offeror shall provide, at a minimum, copies of the following financial information, with the exception of the financial statements identified below. If the entity for which financial statements are submitted files reports with the U.S. Securities and Exchange Commission (SEC), the Offeror may provide electronic links to the most recently filed SEC Forms 10-K, 10-Q, and Form 8-K for all such reporting entities in lieu of hard copy submissions. If the Offeror is a newly formed entity, expressly state that it is or will be a newly formed entity and does not have independent financial information at the time of response to the RFP. If the Offeror is a newly formed entity, it must provide the following financial information for the parent or guarantor entity(ies), which will guarantee the Offeror's obligations under the contract and allow the Government to evaluate financial resources.

- **Financial Statements** – Provide the financial statements and accompanying information listed below. Financial statements shall be prepared in accordance with U.S. Generally Accepted Accounting Principles. Information in the balance sheets, income statements, and statements of cash flow shall be provided in U.S. Dollars. If the entity for which financial statements are submitted files reports with the U.S. Securities and Exchange Commission (SEC), the Offeror shall provide electronic links to the most recently filed SEC Forms 10-K, 10-Q, and Form 8-K for all such reporting entities.
 - **Audited Financial Statements** – Provide audited financial statements for the last three years for the Offeror. The Offeror's fiscal year-end financial statements shall be audited by an independent party qualified to render audit opinions (i.e., certified public accountant). If audited financials are not available, include unaudited financial statements for the entity, certified as true, correct, and accurate by the chief executive officer, the chief financial officer, treasurer, or other authorized signatory (the "Financial Officer") of the entity. Financial statement information shall include the following information:
 - Opinion letter (auditor's report)
 - Balance sheet
 - Income statement
 - Statement of cash flow
 - Footnotes
 - **Interim Unaudited Financial Statements** – In addition to the audited financial statements, provide interim unaudited statements for the above entities. These statements shall reflect the most recent completed fiscal year or the period since the most recent completed fiscal year and shall include the following information:
 - Balance sheet
 - Income statement
 - Statement of cash flow
- **Credit Ratings** – Provide the most recent credit rating(s), if any, associated with the Offeror. If no credit ratings exist, include a statement specifying that no credit ratings exist.
- **Material Changes in Financial Condition** – Provide a letter from the chief financial officer for the Offeror, either (1) providing information on any material changes in the Offeror's financial condition since the date of the last audited financial statement and those that are pending or (2) certifying that no such material changes have occurred. In instances where a material change has occurred or is anticipated, provide a statement describing each material change in detail, the likelihood that developments will continue during the period of performance of the

contract, and the projected full extent of the changes likely to be experienced in the periods ahead. Estimates of the impact on revenues, expenses, and the change in equity shall be provided separately for each material change as certified by the chief financial officer. References to the notes in the financial statements are not sufficient to discuss the impact of

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

material changes. Discuss measures that would be undertaken to insulate FirstNet from any recent material adverse changes, as well as those currently in progress or reasonably anticipated in the future. The following list identifies items that the Government would consider a material change in financial condition. This list is intended to be indicative only and not exhaustive.

- An event of default or bankruptcy involving the affected entity, parent corporation of the affected entity, or any controlled subsidiary or affiliate
- A change in tangible net worth of 10 percent of shareholder equity
- A sale, merger, or acquisition exceeding 10 percent of the value of shareholder equity prior to the sale, merger, or acquisition that in any way involves the affected entity, parent corporation, or financially responsible party of the affected entity
- Adverse changes in credit rating for the affected entity or parent corporation of the affected entity
- Inability to meet material conditions of loan or debt covenants by the affected entity or parent corporation of the affected entity, resulting in the need for a waiver or modification of agreed financial ratios, coverage factors or other loan stipulations, or additional credit support from shareholders or other third parties
- In the current and three most recently completed Offeror fiscal years, the affected entity or the parent corporation of the affected entity (1) incurs a net operating loss; (2) sustains charges exceeding 5 percent of the then shareholder equity due to claims, changes in accounting, write-offs, or business restructuring; (3) implements a restructuring/reduction in labor force exceeding 200 positions; or (4) involves asset disposition exceeding 10 percent of the then shareholder equity
- Other events known to the affected entity that represent a material change in the financial condition over the past three years or that may be pending for the next reporting period (e.g., pending litigation)

L.3.1.5.2 Sources of Funding and Financing

The Offeror shall detail each source of funding or financing used to support the build-out or operation and maintenance of the NPSBN, including the costs, rights, and obligations of each type of funding or financing and details of agreements with funding/financing entities.

L.3.1.5.3 Parent Company Guarantees

The Offeror shall provide details (including terms and conditions) of a guarantee (or equivalent security) from an entity of sufficient financial standing to meet the Offeror's obligations, including disincentive payments, throughout the life of the contract, in the form of a Parental Guarantee Agreement. The Offeror shall submit a fully executed Parental Guarantee Agreement (see Section J, Attachment J-27, Parental Guarantee Agreement) signed by an official authorized to bind the Offeror and the proposed Parental Guarantor. This executed Agreement shall be submitted in Volume I – Business Management, as identified in Section L.3.1.

L.3.1.5.4 Commercialization of Excess Network Capacity

The Offeror shall provide a detailed approach reflecting how the Offeror plans to use Band 14 in its business model, including plans to commercialize the 20 MHz of Band 14 network capacity beyond its sales channel(s) for public safety.

L.3.1.6 Section Six – Delivery Mechanism for State Plans

The Offeror shall provide a clear written description of a Web interface tool for sharing information with governors and/or state decision makers. FirstNet’s objectives for the online delivery mechanism are

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

described in Section J, Attachment J-18, Delivery Mechanism Objectives for State Plans. The Offeror's description of the tools shall include:

- The capabilities, functionality, and information sharing methodology for each type of stakeholder (state, enterprise, and individual)
- How to navigate the online system
- The access control methodology, security, and authentication approach for managing information
- A graphical representation of content provided with the Offeror's proposal relevant to state planning (e.g., coverage maps, device portfolio, service plans)
- The methodology for incorporating additional data or new information in each section of the online system

If the Government determines a demonstration of the online tool is required, additional details will be provided at a later date.

L.3.1.7 Section Seven – Quality Assurance Surveillance Plan

The Offeror shall provide a QASP, in accordance with Section J, Attachment J-6, which defines what FirstNet and the Contractor must do to ensure that the Contractor has performed in accordance with the performance metrics/standards as agreed upon in the contract. Additionally, the QASP is intended to provide a plan to assess the performance of the Contractor in meeting the program's SOO. The Contractor is responsible for management and quality control actions to meet the terms of the contract. The proposed plan shall leverage industry best practices, technology enhancements, and professional expertise. The plan shall employ standard business practices and processes and minimize risk while improving quality of service.

The QASP shall include, at a minimum, a surveillance schedule and clearly state the surveillance method(s) to be used. The QASP must address how the Contractor will measure, assess, manage, and report on the quality of its performance.

L.3.1.8 Section Eight – Deliverables Table

The Offeror shall complete Section J, Attachment J-16, Deliverables Table, noting the deliverables that Offeror will provide following award. The proposed deliverables shall reflect industry best practices and professional expertise. The deliverables shall align with the proposed performance metrics/standards defined in the Offeror's QASP (Section J, Attachment J-9, QASP Surveillance Matrix Template). The proposed deliverables for the successful solution will be incorporated into the final Deliverables Table attached to the contract. The Deliverables Table is a "living document," and the Government may review and revise it on a quarterly basis in coordination with the Contractor.

In addition to any Contractor-proposed deliverables, FirstNet requires specific deliverables to monitor performance and demonstrate value. Those deliverables, which are identified in Section F, Deliverables and Performance, Section F.4.2, FirstNet-Required Deliverables, shall be included in the Offeror's proposed Deliverables Table.

L.3.2 Volume II – Technical

The technical volume shall demonstrate the Offeror has a thorough understanding of coverage and capacity, products, and architecture as they relate to the objectives identified within Section C, SOO, and the associated attachments contained in Section J.

The technical proposal shall not exceed 300 pages in length (150 sheets of paper, double-sided print); this excludes coverage maps and the following Section J attachments from the page limitation: Section J, Attachment J-11, Device Specifications Template; Section J, Attachment J-12, Test Strategy Template; and Section J, Attachment J-17, Coverage and Capacity Template. Section J, Attachment J-17, Coverage and Capacity Template, may be submitted in a soft copy format only as stated herein (flash drive). The technical proposal shall contain the following information and be broken down by the following sections.

L.3.2.1 Coverage and Capacity

The Offeror shall provide a clear, concise description regarding its proposed approach in deploying a network to implement coverage and capacity. This shall include:

- Coverage and Capacity Maps and Statistics
- Radio Access Network (RAN) Solutions and Strategy
- IOC/FOC Milestones for Coverage and Capacity

The proposed solution for coverage and capacity shall address the elements described below according to the IOC/FOC target timeline detailed in Section J, Attachment J-8. Maps submitted by the Offeror shall be based on a bin size no greater than 30 x 30 meters, include Esri shapefiles and MapInfo files (in electronic format), and reference the information contained in Section J, Attachment J-1, Coverage and Capacity Definitions. The statistics shall utilize Section J, Attachment J-17, Coverage and Capacity Template.

The Offeror must complete Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, to demonstrate its ability to meet the objective to provide coverage in all states and territories and to ensure that rural coverage includes partnerships with rural telecommunications providers. The Offeror shall note whether both Band 14 and non-Band 14 coverage are included in each of the 56 states and territories (yes/no), as well as list current and planned partnerships with rural telecommunications providers by state/territory. Lastly, Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, requests tabulation, by state, of the percentage of rural coverage achieved via partnerships with rural telecommunications providers. The Offeror's solution must demonstrate intent to exercise rural telecommunications provider partnerships for at least 15 percent of the total persistent rural coverage nationwide. In the case of anticipated but unexecuted agreements, the Offeror should describe its strategy to mitigate any risks or impediments that may arise should the agreements not come to fruition. While Section J, Attachment J-2, Nationwide and Rural Coverage Compliance Checklist, requests these data by states, the 15 percent coverage factor will be evaluated on a nationwide basis only as stated in Section M, Evaluation Factors for Award.

L.3.2.1.1 Coverage and Capacity Maps and Statistics

The Offeror shall submit all applicable information as defined in Table 2 Coverage Maps Required for Coverage and Capacity. The Offeror shall submit all network statistics, as defined in Table 3 Network Statistics Required for Coverage and Capacity, for each of the 56 states and territories in the Coverage and Capacity Template (Section J, Attachment J-17). The Offeror shall refer to the guidelines provided in Section J, Attachment J-1, Coverage and Capacity Definitions. The Offeror shall describe the details for the network planning design as stated in Section L.3.2.1.2.2, Network Planning and Design, below and the methodologies used to create coverage maps and associated capacity information.

Table 2 Coverage Maps Required for Coverage and Capacity

Level	Band	Phase	Maps Required	Format	Submittal Method
Nationwide	Non-Band 14	FOC	One (1) nationwide map of each file format, depicting coverage by technology: Long Term Evolution (LTE), 3G, 2G, and roaming layers	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via Secure File Transfer (SFT) with Offeror-provided credentials or Offeror-provided portable drive
Nationwide	Band 14	FOC	One (1) nationwide map of each file format, depicting the LTE analysis layers specified in Section L.3.2.1.1.6	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive

* Note: If needed, the Offeror may provide multiple regional MapInfo & Esri (.shp) files that display coverage for smaller areas versus for the entire nation to fit within application and file size limitations. If regional maps are provided, they shall collectively represent nationwide coverage.

The Offeror shall provide the following network statistics in the Section J, Attachment J-17, Coverage and Capacity Template.

Table 3 Network Statistics Required for Coverage and Capacity

Coverage Type	Level	Phase
Non-Band 14 Area Covered **	State/Territory	FOC
Non-Band 14 Population Covered **	State/Territory	FOC
Band 14 Area Covered	State/Territory	FOC
Band 14 Population Covered	State/Territory	FOC
Band 14 Network Capacity	County	FOC

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

L.3.2.1.1.1 Non-Band 14 Area Coverage

The Offeror may propose persistent coverage using non-Band 14 frequencies. This may include all or some of the following technologies, depending on the Offeror’s proposal: LTE, 3G, 2G, and any roaming via the Offeror’s partners. If proposed, the Offeror shall provide a breakdown of offered non-Band 14 coverage, including (as described in Table 2 Coverage Maps Required for Coverage and Capacity) and network statistics (as described in Table 3 Network Statistics Required for Coverage and Capacity), for each proposed technology.

L.3.2.1.1.2 Non-Band 14 Population Coverage

The Offeror may propose persistent population coverage using non-Band 14 frequencies. The Offeror shall overlay its proposed non-Band 14 area coverage map (including the technology layers) with the FirstNet-provided 2010 U.S. Census 1 mile by 1 mile population count map (see Section J, Attachment J-1, Coverage and Capacity Definitions) and provide the proposed output population coverage statistics

(by state/territory) using the Section J, Attachment J-17, Coverage and Capacity Template. Non-Band 14 population coverage may include the following technologies, depending on the Offeror's proposal: LTE,

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

3G, 2G, and roaming (via the Offeror's partners). The Offeror shall provide a breakdown of offered population coverage, including coverage maps and network statistics, for each proposed technology.

L.3.2.1.1.3 Band 14 Area Coverage

The Offeror shall propose persistent coverage using Band 14 frequencies. The Offeror shall provide coverage maps (as outlined in Table 2 Coverage Maps Required for Coverage and Capacity) and network statistics (as described in Table 3 Network Statistics Required for Coverage and Capacity). The Offeror shall provide a proposed persistent coverage for Band 14 that addresses the desired coverage objectives as identified in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.1.1.4 Band 14 Population Coverage

The Offeror shall propose persistent population coverage using Band 14 frequencies. The Offeror shall overlay its proposed Band 14 area coverage maps (including the network analysis layers) with the 2010 U.S. Census 1 mile by 1 mile population count map (see Section J, Attachment J-1, Coverage and Capacity Definitions) and provide the proposed output population coverage statistics (by state/territory) using the Section J, Attachment J-17, Coverage and Capacity Template.

L.3.2.1.1.5 Band 14 Network Capacity

The Offeror shall provide Band 14 network projected demand and capacity statistics at the county level for FOC in Section J, Attachment J-17, Coverage and Capacity Template. Band 14 network capacity is the aggregate proposed design capacity and is computed by summing the average downlink throughput for each cell in a given county. County-based demand—as of 2015—is provided in Section J, Attachment J-1, Coverage and Capacity Definitions, as an input to the Offeror's projected demand at FOC. The Offeror shall describe its proposed process used to forecast Band 14 demand at FOC. The Offeror shall detail the available capacity for public safety and secondary users based on the proposed network. Excess network capacity is defined as capacity not used by Public Safety Entities (PSEs). The excess network capacity shall take into consideration the Offeror's projected highest amount of network usage by public safety during an hour per month as can be derived from the per county demand map in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.1.1.6 Planning Tool Analysis Layers

The Offeror shall provide the following LTE analysis layers for all Band 14 coverage maps noted in Table 2 Coverage Maps Required for Coverage and Capacity:

- Reference Signal Receive Power (RSRP)
- Best Server
- Downlink Signal-to-Interference-Plus-Noise Ratio (SINR)
- Uplink SINR
- Modulation and Coding Scheme (MCS)
- Downlink Average Data Rate
- Uplink Average Data Rate
- Composite Coverage Map

The Offeror shall provide network statistics for each of the LTE analysis layers (with the exception of the RSRP, Best Server, and Composite Coverage Map layers) using Section J, Attachment J-17, Coverage and Capacity Template.

L.3.2.1.2 RAN Strategy and Solutions

The Offeror's proposed RAN strategy and solution shall encompass architecture, design, and deployment strategies that effectively use resources, skill sets, an organizational structure, and tools. The Offeror's proposed approach shall demonstrate the capabilities described below and may include maps, tables showing relevant statistics, and brief descriptions of features and services.

The Offeror shall provide a list of air interface standards and/or non-standards to be implemented in the proposed network to enable communication between Enhanced Node Base stations (eNodeBs) and User Equipment (UE).

Heterogeneous networks (HetNets) may be an integral part of the NPSBN. The Offeror shall describe the types of heterogeneous RANs proposed by the Offeror that will be used by FirstNet UE to communicate with the Core network. The Offeror shall describe any HetNet implementation strategy and proposed deployment scenarios consistent with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline. The description shall include any applicable small cell solutions and associated LTE HetNet architecture, technologies, and equipment.

The Offeror shall describe the network sharing solution for Covered Leasing Agreement (CLA) users, ensuring sharing does not adversely affect public safety users and services. The Offeror shall detail the architecture and service differentiation methodologies for the proposed solution (e.g., Multi-Operator Core Network [MOCN]).

L.3.2.1.2.1 Features and Functionalities Impacting User Experience

The Offeror shall describe the features and services along with any relevant maps, tables, and applicable numeric descriptions. For each spectrum band and technology type the Offeror proposes, the Offeror shall describe the features and services available by proposed covered area type. The Offeror shall describe the user experience capabilities offered within the service area, (e.g., expected throughputs, Quality of Service [QoS], Access Class Barring, capacity thresholds on priority, location services, messaging, data caps, Voice over LTE [VoLTE]). The descriptions shall include supporting maps where applicable.

The Offeror's proposed solution shall describe any nationwide and international roaming capabilities offered to NPSBN users via network partners. The description may include the device frequency and features as well as the roaming network services provided to NPSBN users.

L.3.2.1.2.2 Network Planning and Design

The Offeror shall provide its proposed network planning and design information used for any submissions related to Band 14, including coverage and capacity submissions. This shall include the following documentation:

- **Link Budget** – Detailed link budget analysis sheet that aligns with the Section J, Attachment J-17, Coverage and Capacity Template, Link Budget Parameters tab. The link budget shall account for all assumptions, margins, and gains for both downlink and uplink. It shall be provided for hand-held and high-power UE, maximum allowable path loss, design thresholds, and cell radius for all morphologies (Dense Urban, Urban, Suburban, and Rural).
- **Link Curve** – Detailed link curve along with system simulation data showing the relationship between SINR, code rate, MCS, and throughput.

- **Planning Tool Settings** – Document settings used in the planning tool, including but not limited to Multiple Input, Multiple Output (MIMO) gains; clutter weights/losses; and environment configurations.
- **Geo-data description** – Detailed description of the geo-data used (e.g., clutter, terrain, clutter height, buildings), including but not limited to vintage, source, and resolution.
- **Propagation Models Description** – Detailed description of how the propagation models for planning were generated and if they are calibrated or un-calibrated. If calibrated models are utilized, describe how the models were calibrated.
- **Planning Project and All Supporting Folders** – Copy of the project file used in the Offeror’s planning tool. All supporting files and folders needed to build a project shall be provided with the exception of the site summary data noted below. The project file shall include the analysis generated as well as traffic maps.
- **Site Summary** – Site summary that aligns with the Section J, Attachment J-17, Coverage and Capacity Template, Site Summary tab. A site table shall be provided for the FOC, including a field to identify the site information for each IOC. Site summary data is not required as part of the proposal submittal, but will be required 30 days after award as noted in Section F, Deliverables and Performance.

As part of the evaluation process, the Government reserves the right to request detailed site information (to include all site data for up to two counties per state or territory). If requested, these data are to be supplied using the “Site Summary” tab in Section J, Attachment J-17, Coverage and Capacity Template.

L.3.2.1.2.2.1 Network Design Statistics

The Offeror shall provide its proposed RAN solution for each of the 56 states and territories for each IOC and FOC milestone. The Offeror shall provide the following information in accordance with statistics required in the Coverage and Capacity Template (Section J, Attachment J-17).

- **Downlink SINR Distribution** – Average downlink SINR and distribution by proposed coverage area and population
- **Uplink SINR Distribution** – Average uplink SINR and distribution by proposed coverage area and population
- **MCS Distribution** – Downlink and uplink MCS distribution by proposed coverage area and population
- **Average Downlink Sector Throughput** – Average downlink sector throughput and throughput distribution by proposed coverage area and population
- **Average Uplink Sector Throughput** – Average uplink sector throughput and throughput distribution by proposed coverage area and population

L.3.2.1.2.2.2 RAN Technology Roadmap

The Offeror shall provide IOC/FOC milestone details of its proposed approach for the RAN technology roadmap that includes the applicable technology standards and releases, vendor equipment capabilities, features and services identified for inclusion into the NPSBN, and ways it specifically addresses the RAN public safety needs. The roadmap shall include the target availability date for the items described and shall identify the latest 3GPP release supported. The Offeror shall also provide the proposed RAN hardware, software/feature evolution roadmap, and insight into impacts to RAN nodes, antenna systems and interfaces.

L.3.2.1.2.2.3 NPSBN Vendor Infrastructure Equipment

The Offeror shall describe the proposed RAN vendor portfolio (outlining its proposed equipment suppliers and manufacturers), scope of equipment, and feature interoperability to be included with the NPSBN. Specifications are to be provided where applicable and shall include:

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

- A diagram and description of the LTE base station and sectors, including the antenna system and backhaul components. Identify areas of resource aggregation or redundancy and describe redundancy mechanisms available in the event a radio fails.
- A description of variant eNodeB platforms available in the current architecture, including specifications for each platform.
- Hardware or software techniques utilized to maximize coverage and capacity (e.g., MIMO, carrier aggregation).
- A dimensioning guide for all capacity-dependent hardware and software in the eNodeB. The guide shall describe the traffic load used in the dimensioning calculation as well as any assumptions made for redundancy.
- Solution details if antennae are shared with another frequency band.
- The maximum number of radio bearers supported by each variant eNodeB platform.
- Details for configurations in which a remote radio is involved (e.g., integrated antenna, separate antenna).
- A description of the RAN's congestion management capabilities that would be leveraged in heavy traffic situations.
- A description of which of the 16 3GPP-defined Random Access Resource configurations are supported by each eNodeB platform.
- A description of all RAN security features.

L.3.2.1.2.3 NPSBN Deployment

The Offeror shall describe its proposed nationwide approach to deploying the NPSBN, including any assumptions and considerations used to determine the proposed network offering and service area.

The Offeror shall describe the general design methodologies used to provide indoor and outdoor coverage. Specifically, the Offeror shall articulate with statistics the level of in-building coverage available at each IOC/FOC milestone for Band 14 and any non-Band 14 technologies using Section J, Attachment J-17, Coverage and Capacity Template. The metrics shall include the total available area for each of the 56 states and territories (in square miles), the area covered (in square miles), area covered (in square miles) with useable in-building signal levels, the total available population for each of the 56 states and territories, the population covered, and the population covered with useable in-building signal levels. In areas where in-building penetration from the macro network is inadequate, the Offeror shall describe techniques to enhance in-building coverage. Additionally, the Offeror shall identify which in-building solutions will be served with or without Band 14, including a list of locations for each in-building solution.

The Offeror shall describe the deployment strategy to serve different modes of transportation, such as tunnels, railways, ports and waterways, airports, and roads. The Offeror shall also provide the proposed design, methodologies, sources, and methods used to identify transportation infrastructure coverage requirements and the methodology to determine the appropriate level of indoor, outdoor, and underground service. In addition, the Offeror shall provide details on the approach to integration of in-building solutions with the NPSBN.

The Offeror shall demonstrate in its proposed solution how the capacity is planned beyond serving the public safety addressable market in a given state or territory. The Offeror shall present its strategy for maximizing excess capacity, while taking into consideration the highest amount of network usage by public safety during an hour per month derived from the per county demand map provided in Section J, Attachment J-1, Coverage and Capacity Definitions. The Offeror shall demonstrate the methodology or

the approach in determining the excess capacity that can be preempted during emergency situations. The Offeror shall describe its network hardening strategy (e.g., deployable strategy, selective site hardening, and self-organizing network [SON] for Public Safety Grade [PSG] services). The Offeror's strategy shall meet local building/construction codes and standards.

The Offeror shall concisely explain how it will ensure the RAN components, sites structures, radio equipment, and interconnection are designed and implemented to be resilient against failures that can disrupt services to first responders. The Offeror shall address redundancy strategies, including but not limited to the following:

- **Backup Power** – Provide, on a per state basis, the percentage and location of sites to be configured with backup power systems, the types of backup systems, and the average runtime between service for each of the 56 states and territories. Include detailed plans about portable generators.
- **Resilient Interconnection** – Provide, for each of the 56 states and territories, on a per state basis, the percentage of site infrastructures hardened against backhaul failure with multiple independent interconnections capable of individually handling expected traffic from the wireless facilities.
- **Weatherization** – Provide a strategy for how sites located in areas prone to adverse weather conditions, including but not limited to flooding, storm surges, tornados, earthquakes, hurricanes, ice storms, and wildfires, are addressed.

L.3.2.1.2.4 Network Operations and Performance

This section provides instructions to the Offeror on the information required regarding its proposed approach to network operations and performance. Should the Offeror elect to include a Mobile Virtual Network Operator (MVNO) or MVNO-like model in its solution, details shall be provided pertaining to that solution. These details are not required where an MVNO or MVNO-like model is not proposed.

L.3.2.1.2.4.1 Transition to Operations

The Offeror shall describe the proposed level of assistance provided to first responders to utilize the full capabilities of the NPSBN and any proposed MVNO. This assistance may include training on equipment, features, and services available for normal and emergency operations.

L.3.2.1.2.4.2 MVNO Key Performance Indicators and Acceptance Testing

The Offeror shall describe the end-to-end performance and operations of any proposed MVNO as well as the NPSBN. The description shall include the recent MVNO network performance KPIs and trends as well as the proposed acceptance test plan for the MVNO network performance, UE, and services.

Network performance KPIs include but are not limited to:

- **Accessibility** – Address the probability of an end user being provided with an LTE radio bearer upon request. Include the percentage of successful attempts per overall number of attempts.
- **Retainability** – Address how often an end user abnormally loses an LTE radio bearer during the time that the radio bearer is being used. Include the percentage of abnormal session releases per session time units.
- **Integrity** – Address how the LTE network impacts the service quality provided to an end user or the delay experienced by an end user. Describe throughput (i.e., Internet Protocol [IP] data volume per time) and latency.

- **Availability** – Address when an LTE cell is available for service. Include the percentage of time that the cell is considered available.
- **Mobility** – Address how well the LTE mobility functions are working. Include the handover success rates.

L.3.2.1.2.4.3 Self-Organizing Network

The Offeror shall describe any SON features and services proposed for the Band 14 RAN in terms of self-configuration, self-optimization, and self-healing. The Offeror shall provide the strategy, integration timeline for SON capabilities, and architecture proposed for SON.

L.3.2.1.2.4.4 Deployable Units and Temporary Coverage

The Offeror shall describe the strategy for providing temporary incident-level coverage (Band 14 and non-Band 14) and addressing capacity issues using deployable units, satellite, direct mode, or a combination thereof. The proposed strategy shall describe how temporary coverage and capacity will be provided for areas that are not covered with persistent LTE services. The Offeror shall propose a single, nationwide strategy that describes regional variations. The Offeror shall also provide the following information in the strategy:

- Reference the five National Incident Management System (NIMS) types and planned events, specifically with respect to response time, coverage area, and required capacity.
- List permanent and temporary staging locations (e.g., in the event PSEs mobilize and pre-stage locations for hurricane or wildfire seasons) and proposed quantities of each type of deployable unit.
- Describe how deployable units will be integrated into the macro network and with other deployable units from a RAN perspective to avoid interference and enable handoff communications. Describe how deployable units will be integrated into the Core network and the types of available backhaul.
- Describe the operational aspects associated with each type of deployable, including activation methods, the typical time for deployment from request, operations and maintenance required, and associated costs.
- Describe the envisioned roles and responsibilities from PSEs, FirstNet, and the Offeror with respect to deployables and temporary coverage solutions. Propose a strategy on allowing PSEs to have ownership of deployable assets. Describe the service capabilities (e.g., voice, location, messaging and alerting, throughput, quality of service, priority and preemption) of each type of deployable unit and how the user experience may differ when using deployable units versus services available in areas of persistent coverage.

L.3.2.1.2.4.5 NPSBN RAN Enhancements

The Offeror shall describe the proposed strategy to support necessary network expansion. The strategy shall address coverage, quality, and capacity improvements to the NPSBN and include methodologies and thresholds used to trigger Offeror-defined actions. Improvements may be needed to address the following areas:

- **Coverage** – Extension of coverage to serve new areas (e.g., increase of service area footprint)
- **Capacity** – Additional capabilities to address network congestion (e.g., cell density)
- **Quality** – Improvement of existing capabilities to meet local performance objectives (e.g., strengthening indoor and outdoor coverage)

The Offeror shall provide a proposed framework to facilitate collaboration with local, state, tribal, and federal governments to improve the NPSBN service area and capabilities. The framework shall address shared or independent efforts to align the NPSBN demand and services. The Offeror shall detail the proposed expansion of in-building coverage via government-owned/supplied equipment and use of government property for placement of the Offeror's equipment.

The Offeror shall describe the proposed strategy, methodologies, and decision thresholds needed to improve:

- **Equipment/System Overlays** – Describe the process for repairing or replacing NPSBN equipment due to feature additions or changes in equipment vendors
- **Technology Migration** – Describe the process for system-wide migration (e.g., 4G to 5G).

L.3.2.1.2.5 Early Builder Integration

If the proposed solution includes early builder assets, the Offeror shall describe the proposed early builder assets and how they will be acquired, integrated, and assimilated. The Offeror shall describe the level of effort, strategy, associated risks, and timelines required to acquire, integrate, and assimilate the early builder assets in the respective geographic areas.

L.3.2.1.3 IOC Milestones for Coverage and Capacity

This section provides instructions as it relates to the target milestones set forth in Section J, Attachment J-8, IOC/FOC Target Timeline. Where Section L.3.2.1.1, Coverage and Capacity Maps and Statistics, requires coverage and capacity information at FOC on a per state/territory basis, this section requires details regarding coverage and capacity to be broken out for each of the IOC milestones. For additional instructions regarding the coverage maps and network statistics, see Sections L.3.2.1.1.1 through L.3.2.1.1.4, and apply them to the IOC milestones.

L.3.2.1.3.1 IOC Coverage Maps and Network Statistics

The Offeror shall provide the following LTE analysis layers for all Band 14 coverage maps as noted in Table 4 Coverage Maps Required for Coverage and Capacity.

- RSRP
- Best Server
- Downlink SINR
- Uplink SINR
- MCS
- Downlink Average Data Rate
- Uplink Average Data Rate
- Composite Coverage Map

The Offeror shall provide network statistics for each of the LTE analysis layers (with the exception of the the RSRP, Best Server, and Composite Coverage Map layers) using Section J, Attachment J-17, Coverage and Capacity Template.

Table 4 Coverage Maps Required for Coverage and Capacity

Level	Band	Phase	Maps Required	Format	Submittal Method
Nationwide	Non-Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5	Five (5) nationwide maps of each file format, depicting coverage by technology: LTE, 3G, 2G, and roaming layers.	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive
Nationwide	Band 14	IOC-1, IOC-2, IOC-3, IOC-4, IOC-5	Five (5) nationwide maps of each file format, depicting the LTE analysis layers specified above	Esri shapefiles (.shp) and MapInfo (.grd/.tab) files*	Files shall be provided via SFT with Offeror-provided credentials or Offeror-provided portable drive

* Note: If needed, the Offeror may provide multiple regional MapInfo & Esri (.shp) files that display coverage for smaller areas versus for the entire nation to fit within application and file size limitations. If regional maps are provided, they shall collectively represent nationwide coverage.

The Offeror shall provide the following network statistics in the Section J, Attachment J-17, Coverage and Capacity Template.

Table 5 Network Statistics Required for Coverage and Capacity

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

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

L.3.2.1.3.2 Rural Coverage and Non-Rural Coverage

The Offeror shall indicate the proposed amount of persistent Band 14 rural and non-rural coverage for the nation as a whole and each of the 56 states and territories for the IOC/FOC milestones. The Offeror shall provide this information using the Section J, Attachment J-17, Coverage and Capacity Template. FirstNet-defined rural maps are provided in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.1.3.3 Network Deployment Timing

Using the Section J, Attachment J-17, Coverage and Capacity Template, Sites by IOC_FOC tab, the Offeror shall indicate how quickly the IOC/FOC milestones for Band 14 coverage will be met based on the proposed solution.

The Offeror shall indicate any risks in meeting the proposed deployment schedule.

Where non-Band 14 coverage is proposed, the Offeror shall describe timing for any partner, MVNO, or roaming networks that may be used.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

L.3.2.2 Products and Architecture

Offeror shall ensure that its solution aligns with industry standards as described in Section J, Attachment J-4, System and Standards Views.

L.3.2.2.1 Services

The Offeror shall describe its proposed solution for the following NPSBN services:

- Basic Network Services
- Quality of Service, Priority, and Preemption (QPP)
- Identity, Credential, and Access Management (ICAM)
- Mission-Critical Services

The Offeror shall provide, at a minimum, the following information for each service:

- Service architecture and design documentation
 - 3GPP standards implemented, including version numbers
 - External interfaces described in Section J, Attachment J-4, System and Standard Views
- Roadmap of service features and functionalities according to IOC/FOC milestones
- Design criteria and objectives for services of the NPSBN at the national, state, county, city, and rural levels
- Description of how the metrics outlined in the Offeror’s proposed QASP will be used to monitor and manage the NPSBN service

L.3.2.2.1.1 Basic Network Services

The Offeror shall propose a strategy to provide basic network services to public safety users. If the Offeror includes existing commercial services in its solution, then the Offeror shall demonstrate evidence in achieving quality metrics in current deployments and how it will sustain performance improvements for the proposed basic network services solution.

The Offeror’s solution, whether it is based on existing commercial services or not, shall address the following basic network services:

- **Messaging** – Describe how the solution supports text messaging, Multimedia Messaging Service (MMS), instant messaging, email, voice mail, chat, and Rich Communications Services (RCS)
- **Streaming Video/Audio Services** – Describe how video services will be incorporated and made available to users and applications
- **Voice telephony (VoLTE, VoIP, circuit switched, etc.)** – Describe how the solution supports voice communications throughout the coverage area in cellular and Wi-Fi and by interworking with IP private branch exchange (PBX)/Public Switched Telephone Networks (PSTN)
- **Machine-to-Machine Communications** – Describe how the solution supports device-to-device communications, machine-to-machine communications, and data exchange within the NPSBN as well as to and from external networks
- **IP Multimedia Subsystems Services** – Describe the architectural framework to deliver multimedia services, focusing on interoperability with another carrier’s IP Multimedia Subsystem and third-party IP Multimedia Subsystem application providers
- **Broadcast and Multicast Services** – Describe the proposed broadcast and multicast services for bandwidth-intensive communications

- **Presence Services** – Describe proposed presence and discovery services
- **Location Services** – Describe proposed location-based services with accuracy for x and y coordinates
- **Device Management** – Describe proposed device configurations, accounting and logging, authentication, encryption, key management, lockdown, and status tracking for public safety users
- **Device Authentication** – Provide details on proposed mutual device-network authentication, encryption, and integrity protection for public safety users
- **Lawful Intercept** – Describe how the solution enables the Communications Assistance for Law Enforcement Act (CALEA) to intercept signaling and bearer information for specific users
- **Next Generation 9-1-1 (NG911) Services** – Describe how the solution supports interconnecting and sending information to a Public Safety Answering Point (PSAP)
- **Wireless Emergency Alerts (WEA)** – Provide details on how the solution supports WEA

L.3.2.2.1.2 Quality of Service, Priority, and Preemption

The Offeror shall provide a detailed description of the proposed strategy and design of its QPP solution for the NPSBN, including systems, interfaces, and settings. The solution shall ensure public safety users can access network services during emergencies in spite of network congestion. The Offeror shall describe the following QPP services:

- **QPP States** – Describe how the solution supports moving a cell or cells within the network between distinct operational states. Operational states include static state (i.e., the network relies on its configuration to ensure QPP), dynamic state (i.e., the network takes dynamic response data from public safety users to dynamically control QPP), and controlled state (i.e., a local agency is able to influence the dynamic state through local control).
- **CLA User States** – Describe how the solution supports control of CLA users on the NPSBN. CLA user states include free range (i.e., CLA users have full access to any unused network resource), restricted (i.e., CLA users are limited to a percentage of the network resource), and preempted (i.e., CLA users are removed from the NPSBN for a period of time in a defined geographic area).
- **Emergency User States** – Describe how the solution supports handling immediate peril services and responder emergency services for public safety users.
- **QPP Profiles and Static User Data** – Describe how the solution implements default and emergency QPP profiles for different users with different roles. Define the primary user type and default user roles.
- **Dynamic Data** – Describe how the solution supports dynamically changing data (e.g., user location, user operational status, incident role, incident identifier, incident location, incident severity). These data may be updated via an Application Programming Interface (API) or another method and will be used by the NPSBN to affect dynamic changes to QPP.
- **Application Profiles** – Describe how the solution creates application profiles with static and dynamic application QPP for each application. Application profiles shall include the application type, usage scenario, priority, QoS, preemption, frequency of use, and expected bandwidth.
- **Operational Profiles** – Describe how the solution groups application profiles into operational profiles that can be tailored for each agency.
- **Dynamic QPP Management** – Describe the overall service delivery, management, reporting, and technical approach for addressing FirstNet's QPP objectives.

- **Dynamic Controller** – Describe the solution that interfaces with the various network systems and Local Control to obtain user data (static and dynamic), network utilization, and triggers, as well as drive changes in QPP properties in real time.
- **Priority During Roaming** – Describe how QPP is managed, deployed, and operated while a first responder (priority user) is roaming on a commercial network.

L.3.2.2.1.3 Identity, Credential, and Access Management

PSEs are responsible for managing identity and credentials for first responders. The Offeror shall propose a federated and interoperable ICAM solution that allows public safety agencies to control identity and credentialing of first responders. The Offeror shall address the following areas:

- Describe how the solution improves security and data access for NPSBN users. Describe how the solution allows users of one agency to access data and services provided by a remote agency. Include details of the federated identity interfaces the solution supports and any impacts on an agency's infrastructure, processes, procedures, and applications.
- Describe how public safety agencies will be encouraged to participate in the ICAM solution, including timelines for onboarding and certification. Provide details on how the solution ensures agencies comply with and continue to follow ICAM requirements over time.
- Describe how the solution supports agencies that do not wish to host their own ICAM software and solution. Explain how the solution provides agencies a simple alternative that allows those agencies to fully participate in a federated ICAM solution and share and retrieve information with other public safety users/agencies.
- Describe how the solution supports managing credentials and ensures that credentials are secure and align with the Levels of Assurance (LOAs) as specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-2 and referenced in Section J, Attachment J-4, System and Standards Views. Describe how the solution supports mobile device Single Sign-On (SSO) for both native and Web-based mobile applications. Describe how a user authenticates once and subsequently gains access to the applications using the previously used authentication credential/token. Describe how access to applications and/or services may require step-up authentication when the user provides a credential format/method that does not meet the credential strength requirements of that application/service. Describe how the mobile SSO solution can support different authentication methods and how those align with the defined LOA.
- Describe how the solution supports dynamic attribute-based access control (ABAC) and how applications protected by the solution authorize users before granting access. Provide information on the types of attributes that the solution supports. Include details on how the solution enables local agencies to manage user attributes and access policies.
- Describe how the Offeror proposes to support and evolve the ICAM governance processes and how the Offeror will support agencies adopting ICAM solutions. Provide relevant experiences and characteristics of the Offeror that demonstrate the Offeror's abilities to provide ICAM governance.
- Describe how the proposed solution supports multiple users sharing a device. Provide details on how authentication, authorization, and profiles are managed and supported on shared devices and include details on how each user's data is secured.

L.3.2.2.1.4 Mission-Critical Services

The 3GPP standards body is finalizing several mission-critical services required in the NPSBN to provide public safety users with emergency communication services. The Offeror shall describe its proposed roadmap and product development timing for mission-critical services in accordance with the IOC/FOC milestones outlined in Section J, Attachment J-8, IOC/FOC Target Timeline. Mission-critical services include but are not limited to:

- Enhanced LTE PSG Voice Telephony
- Mission Critical Push-to-Talk
- Broadcast Services for WEA
- Proximity Services (ProSe)
- Mission-Critical Data
- Mission-Critical Machine-to-Machine
- Mission-Critical Location Services (i.e., enhanced accuracy for x, y, and z direction and indoor locations)

L.3.2.2.2 Applications

The Offeror shall describe in detail its strategy and design for its proposed solution for applications, including the following key components:

- The software development methodology and rollout strategy
- The strategy to enhance and update software
- The strategy for soliciting and incorporating public safety input
- The applications release timelines as they relate to Section J, Attachment J-8, IOC/FOC Target Timeline
- Alignment with industry standards described in Section J, Attachment J-4, System and Standards Views
- Alignment with the application security standards described in Section J, Attachment J-10, Cybersecurity

The Offeror shall provide details on how the proposed solution supports performance, availability, reliability, scalability, resilience, manageability, security, and interoperability.

L.3.2.2.2.1 Applications Ecosystem

This section provides instructions related to the applications ecosystem in accordance with SOO Objective #5 in Section C, SOO.

L.3.2.2.2.1.1 Service Delivery Platform

The Offeror shall describe the proposed strategy regarding the following:

- The Service Delivery Platform (SDP) and how it is integrated with public safety APIs, the application development platform, and the network services layer.
- The network services described in Section L.3.2.2.1.1, Basic Network Services, which will be made available to the SDP. Include a proposed schedule of when those services will be made available and how those services will be made available to public safety applications and applications developers.

- The network services capabilities that need to be exposed using a common set of industry standards based on Section J, Attachment J-4, System and Standards Views.
- How the Offeror will develop services and applications policies for various scenarios, such as authorization, congestion management, privacy, API threats, and security. Explain how these policies will be monitored and analyzed.
- Details on any transformation, optimization, tuning, configuration updates, or enhancements that can be completed as a result of network and applications monitoring.
- How the SDP middleware and its application layer QPP policy are integrated with the LTE network layer infrastructure, including policy management.
- Service and application orchestration capabilities that the solution provides and/or capabilities that allow applications to orchestrate and call different services.
- Details on how services and associated applications that consume APIs can be orchestrated for both real-time and non-real-time public safety incidents.

L.3.2.2.2.1.2 Application Development Platform

The Offeror shall describe the proposed strategy regarding the following:

- How the solution supports and allows rapid third-party mobile application development.
- How the solution entices application developers to create applications for the FirstNet applications store.
- Development tools the solution provides and how the tools enhance developer productivity.
- How the solution exposes third-party developers to application development information, tools, Software Development Kits (SDKs), and other development capabilities.
- How the solution enables community support and collaboration tools that the solution provides, including chat, discussion fora, and message boards.
- Mobile application development frameworks the solution supports. Include details of how the framework supports application development and improves developer productivity.
- SDKs specific to developing public safety applications. Include SDK/API documentation. Provide details on APIs that will be exposed to applications. Include details on the network services APIs and additional services APIs, such as map tiles, analytic tools, or other services that the solution will provide.
- Test tools for developers to ensure that applications are free of defects and follow security and mobile application best practices. Note which tools test and/or analyze runtime code or static code. Explain how the tools support application testing throughout the development life-cycle, including before launch and after release.
- How the solution ensures that developers have a high level of confidence that the application will be certified and approved for publication in the FirstNet applications store. Include details on how developers perform application updates and versioning of their applications.

L.3.2.2.2.1.3 Hosting and Cloud Services

The Offeror shall describe in detail how the proposed solution supports cloud-hosted services and applications, providing rationale for why this is beneficial to FirstNet and PSEs. Specifically, the Offeror shall describe:

- How the solution supports hosting applications. Include descriptions of the tools and APIs the solution offers to application developers, Public Safety Enterprise Networks (PSEs), and PSEN

users that are hosting applications or services in the cloud. Include details of the benefits that users receive by hosting applications in the cloud solution.

- How it will provide different cloud services capabilities as they relate to Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Describe how the solution will comply with FirstNet governance on security and standards.
- How the solution supports and provides data analytics and tools to public safety applications. Explain why data analytics are beneficial to FirstNet, PSEs, application developers, and public safety applications.

L.3.2.2.2.1.4 FirstNet Applications Store

The Offeror shall describe its proposed solution pertaining to the following:

- How the solution incorporates new applications into the FirstNet applications store, including the technical details, process, and governance required. Include details on the roles for public safety agencies, FirstNet, application developers, and the Contractor.
- How the solution handles payments and billing for applications and related services. Include details of the payment mechanisms and various pricing models (e.g., monthly recurring charge, one time) the solution supports. Describe how developers can choose the model that best fits their application.
- How the solution supports application change management, including the technical details, process, and governance required. Include details on the roles for public safety agencies, FirstNet, application developers, and the Contractor.
- How the Offeror will support or perform application updates and versioning to software that is provided to agencies and end users through the FirstNet applications store. Describe how the solution ensures that end users are informed of updates and critical patches. For applications provided directly by the Offeror, describe how the solution ensures users are properly trained on the updated software.
- The application life-cycle process, including details for each phase—from creation of the application through its retirement.
- How application customer support is provided to local, tribal, state, regional, and federal users and agencies.
- Additional FirstNet applications store capabilities that allow users to learn about applications capabilities and discover new applications. Include details on how these capabilities align with existing methods and tools that users may be using today.

L.3.2.2.2.1.5 Application Life-Cycle Management

The Offeror shall describe its proposed strategy pertaining to the following:

- The software development methodology that the Offeror and its subcontractors and/or teaming partners follow.
 - Include how feedback from FirstNet and NPSBN stakeholders will be incorporated into future applications ecosystem software releases.
 - Provide the process by which requirements for FirstNet public safety applications are driven through the development and deployment strategy.
- The schedule for each of the applications ecosystem deliverables identified in Section J, Attachment J-8, IOC/FOC Target Timeline. Include each of the capabilities in detail from sections L.3.2.2.2.1.1 through L.3.2.2.2.1.4, including initial release and update strategies.

- New processes for and enhancements to the applications ecosystem to ensure alignment with industry standards, particularly those outlined in Section J, Attachment J-4, System and Standards Views.
- The software update and sustainment strategy, including how to ensure the software continues to evolve and how to address defects. Provide details on how the application environment is agnostic to different mobile platforms, device capabilities, and network capabilities.
- How the application environment is optimized.

L.3.2.2.1.6 Developer and Application Certification

The Offeror shall describe its proposed strategy pertaining to the following:

- The application certification process, including details on the roles and responsibilities for FirstNet, the Contractor, public safety agencies, public safety users, and application developers. Provide details on the technical details, process, and governance required.
- The certification criteria recommended to ensure applications available in the FirstNet applications store are PSG in terms of security, identity management, robustness to malware threats, and resilient performance.
- The different certification levels that the solution supports. Include details on why different certification levels should be used and what the benefits are to FirstNet, public safety users, and application developers.
- The certification timeline for applications, including what circumstances may impact the length of time to certify applications.
- The types of testing required for an application to be certified. Provide details on how the solution tests an application's functionality, scalability, resilience, security, battery drain, and freedom from malware (intentional or unintentional).
- How the solution tests that the application runs correctly on different devices, operating systems, and software versions.
- Details on how the proposed solution will ensure that users maintain the expected level of service of the device and applications when they are on a local network with no backhaul connectivity or are off the network completely.

L.3.2.2.1.7 Application Security

The Offeror shall describe its proposed strategy pertaining to the following:

- How the solution provides application security and ensures that applications and the data used are secure for public safety users.
- How the solution protects data; prevents unauthorized access; and preserves privacy, data integrity, and data availability.
- How the solution will comply with the applicable security guidelines.
- How the solution ensures that the public safety user, agency, and application data are secure at rest, in transit, in use, and on the device.
- How the security posture of local agency applications and services can be viewed and how vulnerabilities can be identified.

L.3.2.2.2 Offeror-Provided Applications

In addition to an applications ecosystem, the Offeror is asked to explain its support for specific applications, including Local Control and a Public Safety Entity Home Page.

L.3.2.2.2.1 Local Control Application

The Offeror shall describe its proposed approach to providing a PSE user interface to each of the network services and Core network services. The Offeror shall describe how this interface enables a PSE to control its administrative and operational environments, including network services, operational support systems (OSSs), and business support systems (BSSs). The Offeror shall describe how the proposed approach addresses the following scenarios:

- An agency has one or more user roles
- An agency has one or more users
- A user has one or more user roles
- A user has zero or more devices
- A user has exactly one profile
- UE may be shared among users, but only one user at a time
- A device has one or more Universal Integrated Circuit Cards (UICCs)
- A UICC has one or more billing services assigned to be usable
- A QPP region has one or more PSEs operating in it
- An agency can operate in zero or more QPP regions

The Offeror shall also describe its support for:

- Event logging and auditing functions
- Onboarding and configuring for the specific needs of an agency
- Accommodation of local input into such topics as cell site locations, network topology, and use of local IP network resources

The Offeror shall describe its proposed strategy pertaining to how it will support the basic local control features listed below:

- Ability to add and remove a device to/from an account
- Ability to add and remove users to/from an account
- Ability to create, modify, and delete user groups and profiles
- Ability to assign users and user groups to user profiles
- Ability to assign applications to user profiles
- Ability to assign devices to users and user groups
- Ability to invoke QPP profiles during a simulated incident
- Ability to blacklist and whitelist applications

The Offeror shall describe how its proposed solution will address the following areas:

- Managing agency-specific policies for users, devices, services, and applications
- Encouraging agency acceptance of applications updates
- Providing local control over which applications may be downloaded and installed on a device
- Planning for “planned events”
- Handling unplanned outages
- Communicating with agencies regarding planned outages and system status
- Eliminating or mitigating outages during planned maintenance
- Tracking outages through resolution and root cause analysis and reporting

- Accepting and processing agency input regarding the planning, design, and construction of the NPSBN within the agency's service area
- Accepting and processing agency input regarding the device ecosystem
- Onboarding and supporting new agencies to the NPSBN and enabling interoperability at all service levels supported

The Offeror shall describe its proposed strategy pertaining to how it will support each of the ongoing network maintenance and expansion processes listed below:

- Describe how a local agency is made aware of service impairment.
- Explain how the Offeror proposes to provide a local agency with near real-time support to allocate network resources during an incident.
- Provide help desk support.
- Provide for a real-time local view of network status, performance, services, and any related trouble ticketing.
- Provide the ability for local agencies to request support and report service issues and impairments.
- Provide the ability to implement end-to-end network change management across each of the 56 states and territories.
- Provide the ability to troubleshoot individual subscriber calls within the Offeror's end-to-end network change management solution.
- Provide an interface into a back end for all operational logs and KPI data for continued service reporting and performance trending.
- Provide the ability for agencies to manage users and control user attributes and roles.
- Provide the ability for users to be recognized by other agencies.
- Provide mobile application management and describe how each agency may control user applications and services.
- Provide mobile device management. Describe how it allows agencies to manage agency and user devices and how it supports a Bring-Your-Own-Device (BYOD) ownership model.
- Describe the application that will be used to manage the priority and QoS of applications and users. Describe how the application allows for the control of user QoS for both voice and data communications.

L.3.2.2.2.2 Public Safety Entity Home Page

The Offeror shall describe its proposed strategy pertaining to the following:

- A customizable home page that provides users with relevant information about their agency and current events and incidents. Describe the home page's timelines for delivery and proposed functionality, including but not limited to the following:
 - Display current status of the wireless network
 - Display critical information of a general nature (e.g., news, weather, traffic)
 - Display critical and/or tactical information of agency-specific information (e.g., incident status, internal alerts, situational awareness data)
 - Support customizable services and data feeds that users can subscribe to, including NPSBN network and service status, agency information, alerts, and basic situational awareness of recent nationwide and local incidents

- How the solution will ensure that the PSE home page meets the needs of public safety agencies and users and how agency/user feedback will be incorporated into new releases of the PSE home page.
- Other forms of status alerting that can be used to notify an agency, such as email, Short Message Service (SMS), Rich Site Summary (RSS), FirstNet status page (as opposed to the PSE status page), and any other such “push” alerts.
- How affected agencies will receive ongoing, timely alerts when an outage impacts them without receiving unnecessary alerts until final resolution.
- How the PSE home page supports ABAC and the ability for local administrators to control what content is displayed and to whom. Explain how the home page can be used to provide access to non-local agency users during mutual aid scenarios.

L.3.2.2.3 Device Ecosystem

The Offeror shall describe the following capabilities associated with the device ecosystem.

L.3.2.2.3.1 Device Portfolio

The Offeror shall list all suppliers, model numbers, operating systems, software configurations, software clients, and embedded applications for the device portfolio. The Offeror shall identify advanced features and limitations across the portfolio for both single and multiple modem configurations. The Offeror shall use the Section J, Attachment J-11, Device Specifications Template, to describe the features and functions that each device in the proposed portfolio supports.

L.3.2.2.3.2 Band 14 Devices

The Offeror shall explain how its proposed device portfolio supports the following configurations for Band 14 devices:

- Smartphones, tablets, and modems that support Band 14 and combinations of other bands and the ability to maintain session continuity when switching from band to band
- In-vehicle routers that support multiple modems, including both Band 14 and combinations of other bands, and the ability to maintain session continuity when switching from band to band
- Vehicular Network Systems built into first responder vehicles that support in-coverage and out-of-coverage rapid response
- A wide variety of cost-effective device types and accessories to meet the needs of first responders
- Machine-to-machine or Internet of Things (IoT) configurations, including low-cost/low-power modems and configurations for video cameras, drone operation, and remote deployment(s)

In addition, the Offeror shall provide details on its proposed strategy pertaining to the following:

- Support for device management, application management, and a security container strategy as they apply to FirstNet standard devices and BYOD scenarios
- The ability to provision standard device and application management, configure standard device security, conduct over-the-air updates for firmware and applications, remove network access, and wipe devices
- For BYOD device support, the approach for onboarding of the device within the agency and systems, setting up the security configuration to support partitioning of FirstNet applications

and data, and removing network access and wiping the FirstNet data and application area of the device

L.3.2.2.3.3 Universal Integrated Circuit Card Management

The Offeror shall present its proposed UICC management program and describe the life-cycle support of profile(s) to operate across multiple networks. The Offeror shall highlight specific modifications that need to be made to current systems and processes to support the needs of public safety users, local control needs, and FirstNet requirements.

L.3.2.2.3.4 Device Management Client

The Offeror shall describe its proposed device management client solution, which shall fully interoperate with a standard Open Mobile Alliance–Device Management (OMA-DM) network solution. The Offeror shall provide documentation of IoT tests being validated with various device management vendors. The Offeror shall identify any extensions to the OMA-DM management and configuration objects needed for its devices and services.

The Offeror shall describe how the proposed device management client solution meets the following requirements with respect to FirstNet’s device management:

- Support for remote management capabilities over the air, including software updates, discovery, device platform configuration, lock, unlock, wipe, security configurations, and other related abilities based on the OMA-DM protocol
- Enablement of local entities to install, update, and manage applications, including managing identification, notification, and removal

L.3.2.2.3.5 Device Approval Process

The Offeror shall supply the following certifications for current devices as part of its device approval process:

- Proof of Federal Communications Commission (FCC)-type certification
- PTCRB test reports after a device has been certified, including but not limited to:
 - TS 36.521 and TS 36.523
 - Uu Interface: 3GPP TS 36.101, 36.104, 36.133, 36.141, 36.201, 36.211, 36.212, 36.213, 36.214, 36.314, 36.321, 36.322, 36.323, and 36.331
 - TS 36.306 UE Radio Access Capabilities
 - TS 31.102 Characteristics of the Universal Subscriber Identity Module (USIM) application
 - TS 31.103 Characteristics of the IP Multimedia Services Identity Module (ISIM) application
 - TS 31.111 USIM Application Tool Kit (USAT)
 - TS 37.571 Positioning
 - CTIA LTE IoT Test Plan
- Code Division Multiple Access (CDMA) certification forum test reports for any device that supports CDMA
- Battery certification reports resulting from the CTIA Battery Certification Program

Further information on the PTCRB test reports can be found in the permanent reference document NAPRD03, *Version Specific Technical Overview of PTCRB Mobile/User Equipment Type Certification*, available on the PTCRB website (www.ptcrb.com).

The Offeror shall identify all open issues and waiver requests. The Offeror shall identify the third-party test laboratory used and/or the mobile network operator laboratory that conducted testing, as well as a point of contact.

The Offeror shall propose an approach to carrier acceptance, referred to as the Device Independent Verification and Validation Test Plan, which can be used to certify public safety functionalities and features of mobile devices before the device is deployed on the NPSBN. The proposal shall provide an acceptance test plan for any of the Offeror's commercial band(s) if applicable to the Offeror's proposed solution.

The Offeror shall provide a roadmap of type certifications and respective standards for future devices.

L.3.2.2.4 Architecture and Infrastructure

The Offeror shall describe a proposed Core network solution, including the Evolved Packet Core (EPC), services, application platforms, and OSS/BSS, that is dedicated for public safety users. The solution shall be capable of integrating with the Offeror's RANs (Band 14 and non-Band 14) as well as state-deployed RANs.

The Offeror shall describe its proposed architecture for the Core network. The Offeror shall demonstrate evidence in achieving quality metrics in current deployments and describe how it will sustain performance improvements for the Core network solution.

The Offeror's description of its proposed architecture shall include but not be limited to the list below, and where applicable, the description shall include operational processes, metrics, and thresholds:

- Architecture descriptions and diagrams, including physical, logical, and geographic architectures
- High-level design criteria, objectives, and components
- Software releases and 3GPP standards (and their respective versions) implemented
- External interfaces to align with Section J, Attachment J-4, System and Standards Views
- Roadmap of network architecture evolution based on IOC/FOC milestones, including components, functionalities, and design criteria evolutions
- Design criteria and objectives utilized for each of the 56 states and territories to maximize system availability, resilience, and reliability
- Failure restoration
- Degradation restoration
- Upgrade(s)/update(s), including the 3GPP upgrade process, to ensure timely deployment of public safety services that are being standardized in the future
- Deployment risk mitigation
- Capacity and traffic growth performance
- Traffic growth and capacity exhaust
- Roaming performance between Band 14 and any other networks
- Core network restoration during disasters and major incidents

L.3.2.2.4.1 Nationwide Core Network Architecture and State Integration

The Offeror shall provide its proposed nationwide Core network architecture and State integration plans.

L.3.2.2.4.1.1 Logical Architecture

The Offeror shall provide system views for all user and control planes for the following platforms, systems, and components:

- All network and service platforms, including SDP, IP Multimedia Subsystem, and EPC systems; transmission systems; location systems; presence systems; and security systems
- All BSSs, including billing, provisioning, asset management, CRM, customer portals, and financial systems
- All OSSs, including network management systems, element management systems, trouble ticketing systems, change management systems, and planned work/workflow systems
- All end-to-end security systems, including firewalls, intrusion detection systems, security gateways, border controls, monitoring, resolution, and investigation systems

L.3.2.2.4.1.2 Covered Leasing Agreement User Integration

The Offeror shall describe its proposed solution to integrate CLA users, including:

- Overall CLA user integration methodology and design
- How the solution ensures there are no adverse impacts to public safety users under normal operating conditions or challenging conditions (natural or man-made)
- Proposed quality metrics applicable to CLA users
- Compliance with 3GPP standards

L.3.2.2.4.1.3 Mobile Virtual Network Operator Strategy

If the Offeror elects to include usage of an MVNO in its proposed solution, then the Offeror shall provide its strategy for the MVNO network, including:

- A schedule of MVNO service availability to public safety
- Proposed capabilities to be offered under the MVNO
- A migration plan from the MVNO network to the NPSBN
- The quality specification and user performance of services and functionalities of the MVNO network
- A methodology of interworking between the NPSBN and MVNO network, including key considerations, parameters, and quality metrics
- A roadmap of MVNO strategy milestones that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline

L.3.2.2.4.1.4 Key Core Network Locations

The Offeror shall describe its proposed solution, including the information below, for key Core network locations (e.g., datacenters; switching, routing, and transmission hubs).

- Layout and configuration of Core locations
- Core location infrastructure, including mechanicals; fire suppression; racks; cabinets; primary power; back-up power; and heating, ventilation, and air conditioning (HVAC)
- Core location TIA-942 classification
- Core location type (e.g., owned or leased space, leased rack)
- Physical security access and egress policies

- Entrance facility redundancy and spatial diversity (e.g., power, transmission)
- Geographic zoning classification

L.3.2.2.4.1.5 Network Specifications, Design Criteria, and Operational Metrics

The Offeror shall provide a proposed strategy regarding network specifications, design criteria, and operational metrics (to be provided in the Offeror's proposed QASP; see Section J, Attachment J-6, Quality Assurance Surveillance Plan) for the following:

- Application platforms and enabling systems, such as IP Multimedia Subsystem, EPC systems, transmission systems, and OSS and BSS interfaces
- Non-standard or specialized equipment
- External network interconnection points such as PSTN, PSEs, Internet Service Providers (ISPs), and WSPs
- NPSBN, OSS, and BSS quality
- RAN/Core integration including the operations and maintenance interfaces between RANs and the Core in support of the NPSBN Services Management Center (SMC) (as described in Section L.3.2.2.5.3, Services Management Center)

L.3.2.2.4.1.6 Session Continuity

The Offeror shall describe its proposed strategy pertaining to how it will provide session continuity between the NPSBN and other networks for voice, data, and streaming sessions as well as signaling sessions. The Offeror shall describe how its solution achieves service continuity for each IOC and FOC milestone.

L.3.2.2.4.1.7 Roaming Strategy

The Offeror shall describe its proposed roaming strategy, including its solution for roaming between the NPSBN and any partner networks as well as other wireless systems while maintaining session continuity and appropriate QPP parameters. The Offeror shall provide a roadmap of roaming strategy milestones that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.1.8 Roaming Partner Integration

The Offeror shall provide its proposed approach for integrating roaming partners. The solution shall address how session continuity and appropriate QPP parameters will be impacted as users roam between Band 14 and other non-Band 14 networks.

L.3.2.2.4.1.9 IP Strategy

The Offeror shall provide its proposed IP strategy as it relates to IPv4 and IPv6. The Offeror shall outline its solution to distribute, assign, maintain, and manage public and private IP addresses. The Offeror's strategy shall include a roadmap to IPv6 that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.1.10 Heterogeneous Network Integration

The Offeror shall describe its proposed solution to integrate multiple networks (i.e., MVNO, Core, roaming partners, state-deployed RANs), as applicable, to form a seamless NPSBN. The Offeror shall outline its solution to maintain and manage this HetNet as well as ongoing network additions, upgrades,

updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its HetNet integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2 Transmission Systems Strategy

The Offeror shall provide a proposed transmission systems strategy that describes how the Offeror will support RAN backhaul, backhaul aggregation, a nationwide backbone transmission system and associated transmission security, routing methodologies, and service prioritization, including end-to-end QoS and priority integrity across LTE and transport layers. All integrated networks—e.g., MVNO, Core, roaming partners, and state-deployed RANs, as applicable—shall form a seamless interoperable NPSBN. The Offeror shall outline its solution to maintain and manage these transmission systems, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its transmission systems strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.1 RAN Backhaul Architecture, Topology, and Synchronization

The Offeror shall provide its proposed RAN backhaul architecture, topology, and synchronization approach across integrated networks (i.e., MVNO [if applicable], Core, roaming partners, and state-deployed RANs) and describe how it enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage RAN backhaul architecture, topology, and synchronization systems and components, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its RAN backhaul architecture, topology, and synchronization strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.2 RAN Backhaul Aggregation Transport Network

The Offeror shall describe the proposed architecture and design of its RAN backhaul aggregation transport network. The Offeror shall describe how it operates across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs) and how it enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage the RAN backhaul system aggregation transport network system and components, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its RAN backhaul aggregation transport network that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.3 National Transmission Network

The Offeror shall describe its proposed strategy pertaining to its national transmission network, which shall operate across any integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how the national transmission network enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage the national transmission network, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its national transmission network strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.4 Transport Security

The Offeror shall describe its proposed strategy pertaining to its transport security approach across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage transport security systems and components, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its transport security strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.5 Routing and Diameter Routing Agent Strategy

The Offeror shall describe its proposed strategy pertaining to routing and Diameter Routing Agent (DRA) approach across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage routing systems and components including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments and removals. The Offeror shall provide a roadmap for its routing and DRA strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.2.6 Transport Service Prioritization

The Offeror shall describe its proposed strategy pertaining to its transport service prioritization approach across integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage the transport service prioritization, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its transport service prioritization strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3 Interconnection and Interworking

The Offeror shall describe its proposed approach to interconnection and interworking, including how it supports state-deployed RAN backhaul aggregation integration, PSEN and PSAP integration, PSTN integration, and Public Land Mobile Network (PLMN) integration with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage these connected systems, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its interconnection and interworking strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.1 State-Deployed RAN Integration

The Offeror shall describe its proposed approach to integrating state-deployed RANs with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage connections with state-

deployed RANs, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its state-deployed RAN integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.2 PSEN and PSAP Integration

The Offeror shall describe its proposed approach to integrating PSENs and PSAPs with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation of the NPSBN. The Offeror shall outline its solution to maintain and manage these PSEN and PSAP connections, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its PSEN and PSAP integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.3 PSTN, ISP, and Peering Integration

The Offeror shall describe its proposed approach to integrating PSTN, ISP, and peering networks with the Core network across all integrated networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage connections with PSTN, ISP, and peering networks, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its PSTN, ISP, and peering integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.4 PLMN and Roaming Partner Integration

The Offeror shall describe its proposed approach to integrating PLMN and roaming partners with the Core network across all integrated networks (i.e., MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how the approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage these connections, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its PLMN and roaming partner integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.3.5 Support for Land Mobile Radio Network Integration (if proposed)

If the Offeror's proposed solution includes future plans for Land Mobile Radio (LMR) integration, the Offeror shall describe its approach, if proposed, to integrating LMR networks to the Core network across all integrated networks (i.e., MVNO, Core, roaming partners, and state-deployed RANs). The Offeror shall describe how this approach enables seamless network implementation and operation. The Offeror shall outline its solution to maintain and manage these connections to the LMR network, including ongoing network additions, upgrades, updates, configuration changes, rearrangements, assignments, and removals. The Offeror shall provide a roadmap for its support for LMR Network integration strategy that aligns with the IOC/FOC milestones described in Section J, Attachment J-8, IOC/FOC Target Timeline.

L.3.2.2.4.4 Public Safety Grade

The Offeror shall describe its solution to achieve PSG services for network reliability, resiliency, redundancy, environmental factors, and operational management approach.

L.3.2.2.4.4.1 Network Reliability

The Offeror shall describe its proposed network design and how it will ensure network reliability. The Offeror shall provide a benchmark for network reliability against existing commercial wireless operators.

L.3.2.2.4.4.2 Network Resiliency

The Offeror shall demonstrate its ability to provide and maintain an acceptable level of service as defined in SOO Objective #7, User Service Availability, in the face of natural disasters, faults, and other challenges to normal operation. The Offeror shall outline the solution and its ability to maintain and improve network resiliency for the NPSBN.

L.3.2.2.4.4.3 Network Redundancy

The Offeror shall describe its proposed solution to increase service availability through local and geo-redundancy solutions. The description shall include proposed methods for all layers of the network and associated quality improvement metrics gained as a result of this solution, especially in highly vulnerable key network nodes supporting mission-critical infrastructure.

L.3.2.2.4.4.4 Environmental Factors

The Offeror shall describe actions being taken in the design and implementation of the NPSBN to mitigate environmental factors that could adversely affect the performance of the NPSBN. The Offeror shall describe its proposed solutions for different regions impacted based on specific environmental factors (e.g., earthquakes, tornados, hurricanes, floods, fire) that could adversely impact the performance of the NPBSN (e.g., loss of core switch, loss of multiple sites covering an area, loss of large capacity connectivity). The description shall address each of the 56 states and territories.

L.3.2.2.4.4.5 Operational Management Approach

The Offeror shall describe how its proposed operational management approach is proactive and results in a continual improvement of network performance, services, and support for public safety users. The Offeror shall outline how it will report and communicate the network status, network impairments, and resolution status at a detail meaningful to local, state, and federal users. The Offeror shall describe past experience in proactive maintenance and introduction of new features, functionality, and applications without impacting user services.

L.3.2.2.4.5 Network Implementation

In this section, the Offeror shall describe various elements of network implementation, including integration with any partners or MVNOs, naming and identifying network nodes, design assumptions, numbering plans, number portability, and project plans.

L.3.2.2.4.5.1 Integration with Partners

The Offeror shall describe its proposed approach for integrating the NPSBN with partners. The integration includes all involved networks (i.e., any MVNO, Core, roaming partners, and state-deployed RANs).

L.3.2.2.4.5.2 Network Naming and Identification

The Offeror shall provide its proposed design/plan for naming and identifying network nodes for the NPSBN. The Offeror shall describe how this approach facilitates seamless implementation and operation of the network. The Offeror shall provide an approach for identifying public safety devices, RAN equipment, Core network equipment, telephone numbers, tracking areas, proximity-based services, LTE/Wireless LAN (WLAN) interworking, Evolved Multimedia Broadcast Multicast Service (eMBMS) service, group multicast calls, and group broadcast calls. The Offeror shall describe its naming and identification approach for at least the following items:

- International Mobile Subscriber Identity (IMSI)
- PLMN Identifier
- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Tracking Area Identifier (TAI)
- Access Point Name (APN)
- Global Unique Temporary UE Identify (GUTI)
- Global Unique MME Identify (GUMMEI)
- Cell Radio Network Temporary Identifier (C-RNTI)
- Packet Data Network Identity (PDN ID)
- Evolved Packet System (EPS) Bearer Identifier
- E-UTRAN Radio Access Bearer (E-RAB) Identifier
- Linked EPS Bearer Identifier
- Tunnel End Point Identifier
- International Mobile Equipment Identity (IMEI)
- Access network discovery and selection function (ADNSF) Server Name
- Temporary Mobile Group Identity (TMGI)
- ProSe Application ID
- Fully Qualified Domain Names for Security Gateway and Operations, Administration and Management (OAM) Systems

L.3.2.2.4.5.3 Design Assumptions

The Offeror shall provide the assumptions employed when designing the NPSBN network in accordance with Section L.2.6, Assumptions, Conditions, and/or Exceptions. The assumptions shall clearly identify responsible owners. The Offeror shall clearly identify any impact to quality metrics defined in the Offeror's QASP in case assumptions differ from implementation. The Offeror shall provide a three (3) to five (5) year forecast of assumptions that are relevant to the NPSBN network design.

L.3.2.2.4.5.4 Numbering Plan

The Offeror shall provide its proposed numbering/addressing schema for public safety devices. The Offeror shall provide the Integrated Services for Digital Network (ISDN) numbering plan, which complies with U.S. regulations, to assign public safety devices. The Offeror shall provide a schema on how device numbering will be mapped to user identities to support ICAM. In addition, the Offeror shall provide a network address approach for packet data communication between public safety devices and mobiles devices on other networks. The Offeror shall describe how the numbering and addressing plan supports public safety devices roaming in other PLMNs. The Offeror shall address how its approach supports both IPv4 and IPv6.

L.3.2.2.4.5.5 Project Plan/Schedule

The Offeror shall provide a proposed project plan and schedule for the implementation of the NPSBN. This includes but is not limited to RAN, Core, network services, transport network, applications, OSS, and BSS. The Offeror shall identify any variances with Section J, Attachment J-8, IOC/FOC Target Timeline, and the reasons for those variances. The Offeror shall provide a roadmap for the launch of the NPSBN that aligns with the IOC/FOC milestones.

L.3.2.2.4.5.6 MVNO to NPSBN Core/RAN Migration

Should the Offeror elect to implement an MVNO or MVNO-like model, then the Offeror shall describe its proposed approach to migrating public safety users from the MVNO to the NPSBN. This approach may include a number of phases (some of which are identified in Section J, Attachment J-8, IOC/FOC Target Timeline) but shall at least include migration to the Core network, NPSBN applications ecosystem, NPSBN devices, NPSBN services, and the scheduled rollout of the NPSBN RAN network.

L.3.2.2.4.5.7 Mobile Number Portability

The Offeror shall describe its proposed approach to mobile number portability. The Offeror shall describe how it will change the IMSI or mobile service provider without changing the ISDN number allocated to a public safety device. The Offeror shall provide the time frame of the porting process in accordance with Section J, Attachment J-3, FCC TAB RMTR. Support for number portability where an MVNO model is proposed shall also be described.

L.3.2.2.5 Operations

This section addresses proposed network and service operations, business and operational support systems, SMC, and service availability.

L.3.2.2.5.1 Network and Service Operations

The Offeror shall provide a clear, concise description that demonstrates how its managed services will meet the stated service availability objectives, as identified in Section C, SOO, for the NPSBN, including all services and applications provided. The Offeror shall describe its proposed strategy pertaining to the following:

- How an integrated service support model that is aligned with the Information Technology Infrastructure Library (ITIL®) or commercial equivalent will be delivered. The model shall include configuration, change, incident, and release management processes.
- The support personnel and systems used in the operations and fault diagnosis of the NPSBN. This shall include descriptions of support personnel and escalation procedures used in the investigation and resolution of anomalies, degradations, and impairments. Describe the tools used to verify call flows and messages between Core and RAN subsystems and test equipment to further diagnose or provide detection of system anomalies or degradations.
- Its NIMS processes and how they enable effective communications with the incident commander and emergency operations center (EOC) in times of localized, regional, or national emergencies or incidents. These shall be consistent with Federal Emergency Management Agency guidelines and best practices and include:
 - A description of specific support organizations that are stood up in times of localized, regional, or national incidents that shall interface, coordinate, and support on-site incident commanders and EOCs

- Reporting and communication practices to relay status and performance levels for local, state, and federal users
- Reporting and communication practices to relay impairments and resolution status levels for local, state, and federal users
- Release management processes to introduce features, functionality, and applications into the NPSBN without impacting user services.
- Business continuity management processes, including provisions for disaster recovery and major event support to local, state, and federal agencies.
- Ongoing service-level management processes that provide a continued baseline of system and per service performance, including proactive improvement plans for increased performance, service, and support of NPSBN users. Include descriptions and examples of how service levels (meaningful to local, state, tribal, and federal public safety users) are reported to FirstNet.
- Availability management processes, including ongoing analysis of availability failures, contingency planning, and other activities and processes to ensure service availability objectives are met.
- Change management processes to support life-cycle NPSBN production changes and upgrades including software, hardware, asset deployment, and new asset integration. These shall include descriptions of how proposed changes and upgrades are submitted for review, approved, scheduled, and communicated to local, state, tribal, and federal agencies.
- Capacity management processes to meet current and future NPSBN objectives. These shall include descriptions of how the Offeror manages NPSBN utilizations, including computing, storage, network, and application sizing to ensure ongoing service levels.
- The national and local support structure to provide on-site support for both reactive and proactive configuration, maintenance, and monitoring activities. This shall include network optimization activities and quality assurance activities for the NPSBN.
- Protocols and processes to address state and local support of natural disasters and major events requiring deployable assets. The description shall include quantities of deployable assets and the default distribution of assets to support rapid response; procedures to request assets (both proactively and reactively); and deployment, operations, and support during such events.

L.3.2.2.5.2 Business and Operational Support Systems

The Offeror shall provide a clear, concise description that demonstrates how its proposed BSS and OSS will meet the stated objectives, as identified in Section C, SOO. The Offeror shall describe the following:

- The systems and interfaces in the application service to BSS and OSS. Include details on how the applications ecosystem provisions, charges (e.g., one-time, monthly recurring cost), and reports based on usage.
- The flexibility of the billing systems to define new profiles based on the agency usage billing models, throttling profiles, access to services/profiles, account types, and local control.
- The user, device, service, and application provisioning and management system(s) that enable and disable capabilities and provide information to the BSS in support of user adoption.
- The process utilized to ensure all regions are in sync with the billing and operational support system(s), including deployable units. Include how these systems report hardware, software, subsystem dependencies, and configuration-level consistencies or discrepancies.
- The back-end systems and interfaces that support the storage of historical system operational logs, system KPIs, performance metrics, billing transactions, and all other key files or logs needed for historical trending, records retention, and other performance management needs.

- The OSS's real-time ability to provide event-based monitoring correlating the different NPSBN subcomponent or network element alarming, including radio frequency systems, microwave backhaul, satellite backhaul, fiber backhaul, networking components, regional and Core LTE components, and application servers.
- The OSS's ability to provide real-time, performance-based monitoring and reporting around user onboarding and provisioning, user service experience, and individual NPSBN component performance that can be meaningful and applicable to an agency, tribe, or region.
- The capabilities and features of an electronic delivery mechanism(s) and format(s) that FirstNet personnel may use to conduct real-time and historical monitoring and investigation of network and service health, as well as usage and performance trending and analysis.
- The CRM systems used to capture and report on a user's life-cycle on the NPSBN. Include descriptions of how the system captures billing history, customer care interaction, current and historical performance, and technical support tickets and statuses for an individual user and agency.
- The trouble ticketing system for users reporting a degraded user experience on the NPSBN. Include descriptions of the workflow in investigating and resolving user issues; communication of current status or resolutions; and system's ability to detect, correlate, and alert out larger issues based on incoming ticket volume.

The Offeror shall show how a state that assumes responsibility for deploying its own RAN can also use the BSS and OSS effectively.

L.3.2.2.5.3 Services Management Center

The Offeror shall provide a clear, concise description that demonstrates the proposed structure of its SMC. The Offeror shall describe the following:

- The SMC location(s) and structure(s) that support the various network and service support functions, including applications, billing and provisioning, content services, devices, network (Core, RAN, Wide Area Network [WAN]), security, surveillance, and service desk.
- Technical support staff and resources available among each network and service function and how service troubleshooting is orchestrated by the SMC for varying levels of service. Detail how the SMC is made aware of all on-call staff spanning local/on-site locations to Core/national locations.
- The process of how public safety users originate a request or service issue into the SMC and how staff correlate and assess if a larger issue affecting users exists.
- Network and element management systems that provide real-time monitoring and dashboards of the end-to-end network. Detail how individual alarms are rolled up and correlated to service-based events. Include how SMC staff members are effectively prepared to respond, resolve, or route events to the appropriate next tier of support.
- How incidents are effectively managed and communicated based on the severity and location. Describe how an incident life-cycle is managed and effectively handed off between SMC shifts.
- KPIs around messaging of service status as well as its effectiveness in the identification and resolution of service degradation issues.
- Training plan for all SMC staff.
- Continuity staffing plan for key SMC positions.

L.3.2.2.5.4 Service Availability

It is FirstNet’s objective to acquire services of a network designed to operate during natural and man-made disasters with restoration of services to the NPSBN taking precedence over other services. Availability is to be measured based on user data sessions and calculated as a percentage of successful user data sessions relative to attempted user data sessions for the reporting area and time period.

The Offeror shall propose how data sessions (successful, unsuccessful, and attempted) will be measured and reported. The Offeror shall also propose definitions of geographic reporting to ensure users and their agencies receive reliable service. The Offeror shall include its overall network design and operations strategy for providing high availability with special attention to those areas identified in Section J, Attachment J-1, Coverage and Capacity Definitions.

L.3.2.2.6 Security

The Offeror’s proposed solution shall encompass the design, architecture, and operational and testing plans with respect to cybersecurity of the NPSBN.

L.3.2.2.6.1 Public Safety Security

The Offeror shall provide a clear, concise description regarding its proposed approach to protect the network from cyberattack while maintaining reliable access. This description shall include but is not limited to the following considerations:

- **Usability** – Provide details on how the proposed solution will establish protective mechanisms that function effectively without adversely affecting network access.
- **Mission Primacy** – Outline and document how the proposed security mechanisms ensure uninterrupted or minimal degradation to the public safety mission.
- **Operational Security** – Provide details on how public safety data are protected while in transit and at rest.
- **Responder Safety** – Provide details on how the proposed solution will ensure the ability to request emergency assistance from first responders in mission performance or under immediate peril.
- **Reliability/Resiliency** – Provide details on how the solution will ensure service availability of the NPSBN.
- **Data Protection** – Provide details on how the proposed solution will safeguard Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Services (CJIS), and Payment Card Industry (PCI) data.
- **End-to-End Protection of Data** – Provide details regarding the end-to-end protection of data by using encryption or other related methods and technologies.
- **Privacy** – Provide details on how the proposed security mechanisms across the NPSBN will ensure protection of personal data traversing the NPSBN.
- **Authentication** – Provide details on proposed authentication methods and technologies to ensure consistent access. The solution shall include, at a minimum, a federated ICAM solution with associated multifactor authentication.
- **Multi-Layer Security** – Provide details on how the proposed solution will permit individual PSEs to layer local security requirements onto the NPBSN for maximum flexibility within their respective jurisdictions.

- **Federal Information Security Management Act (FISMA) Compliance** – Provide details on how the proposed solution will permit relevant entities to ensure compliance with applicable requirements under FISMA when using the NPSBN.

L.3.2.2.6.2 Architecture Security

The Offeror shall provide a clear, concise description regarding its proposed approach to secure and protect the architectural components of the NPSBN within the context of public safety and accepted industry best practices. The description shall include but is not limited to end-to-end security management and logging, private encryption key management infrastructure, security policies and practices, fraud prevention and revenue assurance, network address translation support, protection between users, signaling storms, rogue or spoofed devices, HetNet support, Domain Name System (DNS) security, messaging security, IP Multimedia Subsystem security, BSS, OSS, mobile Virtual Private Network (VPN) support, business continuity and disaster recovery, IP infrastructure network elements, security hardening, cybersecurity, governance, cyber supply chain, insider threat mitigation, cloud environments, virtualization, software-defined networking, and VoIP spam. In addition to these elements, the Offeror shall include the following:

- **Security Integration and Testing** – Provide, at a minimum, the methods and approach for onboarding software/hardware and applying updates with associated testing to ensure optimal functionality within the approved security architecture. This includes mitigation strategies for required updates that may potentially introduce operational impacts.
- **Architectural Considerations** – Describe how the solution meets the requirements specified in Section J, Attachment J-3, FCC TAB RMTR.
- **3GPP Standards** – Describe how the solution adheres to 3GPP standards for cellular communication for both voice and data.
- **GSM Association (GSMA) Specifications** – Describe how the solution meets applicable GSMA specifications as outlined in Section J, Attachment J-3, FCC TAB RMTR.
- **Transport** – Provide details regarding the protection of data while in transit through appropriate use of encryption, access control, and other accepted policies and technologies. This includes data traversing external interfaces.
- **Domains** – Provide details regarding effective end-to-end protection and security of the indicated domains, including but not limited to:
 - RANs within each state and territory (either FirstNet-deployed or state-deployed)
 - Backhaul network, including eNodeB to regional aggregation points
 - Aggregation network, including aggregation of traffic in a region
 - National transport networks, including network connections to regional and national Core sites
 - EPC
 - BSS
 - OSS
 - Applications ecosystem
 - IP Multimedia Sub-System
 - Value-added services
 - Messaging services
 - PSE network connectivity
 - NPSBN cloud environments

L.3.2.2.6.3 Device Security

The Offeror shall provide a clear, concise description regarding its proposed approach to protect various aspects of the device ecosystem. This includes but is not limited to securing the operating system architecture, authentication mechanisms used for users and applications, embedded applications, mobile device management (MDM) and mobile application management (MAM), PSE-managed whitelist/blacklist, digital signatures of applications, and device security, including for BYOD, applications, and wearables.

L.3.2.2.6.4 Applications Security

The Offeror shall provide a clear, concise description regarding its proposed approach to protect elements of the applications used within the NPSBN. This description shall include but is not limited to the applications ecosystem, APIs, application software development life-cycle, application security certification, application vulnerability management, application developer certification, user logging, end-to-end application, application-specific port monitoring and validation, application and device security, data loss prevention, and secure application coexistence.

L.3.2.2.6.5 Identity, Credential, and Access Management Security

The Offeror shall provide a clear, concise description regarding its proposed approach to effectively secure ICAM. The description shall include, at a minimum, the following key elements:

- ICAM with federated identity from PSE networks
- Identity Assurance:
 - User to Device – PSEs may share a device between several first responders, necessitating the agency to identify which user has the device
 - Device to Network – LTE authentication
 - Network to Application – Identity management
 - Network to PSE Network – Identity management
 - User to Application – Identity management
 - User to PSE Network – Identity management
- Authorization
- Credentialing

L.3.2.2.6.6 Cryptographic Employment

The Offeror shall provide a clear, concise description regarding its proposed approach to effectively mitigate attack vectors against the IP-based infrastructure by employing encryption.

L.3.2.2.6.7 Public Safety Enterprise Network Security

The Offeror shall provide a clear, concise description regarding its proposed approach to formulate and implement minimum security standards to enable Public Safety Enterprise Networks to connect to the NPSBN.

L.3.2.2.6.8 Cybersecurity Life-Cycle

The Offeror shall describe its proposed cybersecurity life-cycle, including, at a minimum, how the Offeror will identify vulnerabilities and threats, determine risks arising from threats and vulnerabilities, prioritize risks to determine which warrant associated controls to address threats or vulnerabilities,

specify and implement controls to address or mitigate those threats and vulnerabilities, assess the effectiveness of controls, and monitor the security of the system.

L.3.2.2.6.9 Cybersecurity Systems Engineering

The Offeror shall provide a clear, concise description regarding its proposed approach to effectively ensure sustained security of all NPSBN environments. At a minimum, the Offeror shall:

- Enumerate operational policies and procedures to ensure that the cybersecurity system engineering approach is followed at all levels.
- Include repeatable processes that are executed continuously during the development and evolution of the NPSBN.
- Ensure cybersecurity engineering is considered in all decisions, designs, and actions.
 - Ensure the network is used only by authorized personnel.
 - Ensure the network and its users are protected from others, including external adversaries and insider threats.
 - Ensure the cybersecurity program is robust.
 - Ensure the design of the network and its components are secure by facilitating a cybersecurity assessment and utilizing resilient design principles.
 - Establish processes for application security policies and procedures, and distribution of applications to be used on the NPSBN.

L.3.2.2.6.10 Risk Management

The Offeror shall provide a clear, concise description regarding its proposed risk management methodology, which should be executed continuously during the system development life-cycle and throughout the life of the contract and the NPSBN. The methodology may be based on or enhanced by a number of existing models, such as the NIST Risk Management Framework or the ISO 27000 series. The methodology shall include, at a minimum, the following:

- Asset identification
- Risk impact analysis
- Threat assessment
- Risk mitigation
- Security control selection and deployment
- Risk mitigation operations and maintenance

L.3.2.2.6.11 Cybersecurity Incident Response

The Offeror shall provide the Government with a documented Cybersecurity Incident Response Plan that includes but is not limited to computer security monitoring to rapidly detect incidents, vulnerability detection and analysis, log collection and analysis, tracking and reporting of incidents, and restoration of information technology (IT) operations after an incident occurs. The plan shall include specific technical processes, techniques, checklists, and forms to be used by the incident response teams. The Contractor shall document methods to report and escalate incidents to FirstNet in a timely fashion.

The Offeror shall provide a clear, concise description regarding its proposed approach to cybersecurity incidents. At a minimum, the Offeror shall describe how it will:

- Coordinate the notification and distribution of a cybersecurity incident.

- Mitigate the risk of an incident by minimizing disruptions.
- Notify the Contracting Officer if it appears that the mitigation will have an associated cost.
- Assemble security staff to conduct a threat analysis and resolve the incident.
- Take reasonable steps to mitigate the effects and minimize any damage resulting from the incident.
- Monitor system logs for application to the incident.
- Categorize all cybersecurity incidents per policy and procedure and report them within specific time frames.
- Define and capture metrics that will be used for reporting capability.
- Provide a post-mortem for each incident associated with an actual cyberattack in a format agreed upon by FirstNet and the Contractor.
- Provide an after action report for any incident that occurs due to inadvertent actions by authorized operations and maintenance personnel in a format agreed upon by FirstNet and the Contractor.
- Record and log all cybersecurity incidents into an electronic format.
- Report all cybersecurity incidents based on incident severity, as directed in standard operating procedures that will be developed jointly between FirstNet and the Contractor.

L.3.2.2.6.12 Security Operations Center

The Offeror shall provide a clear, concise description regarding its proposed security operations center. This shall include technologies employed, reports provided, logging approach and related forensic analysis of those logs, and incident response capability, as well as mitigation processes and related escalation procedures and criteria. The Offeror shall describe how it will, at a minimum, do the following:

- Collect, maintain, and share information about threats to network infrastructure, devices, data, and applications.
- Provide 24/7/365 cybersecurity monitoring of network infrastructure, devices, data, and applications.
- Provide monitoring and analysis of user, system, and network access.
- Assess the integrity of the NPSBN and associated data.
- Establish a baseline for network activity and utilization.
- Recognize and analyze activity patterns that are indicative of an incident or intrusion.
- Analyze logs for abnormal patterns.
- Establish information sharing and collaboration that integrates and disseminates information among critical infrastructure partners.
- Process, generate, and post suspicious activity reports.
- Provide assessment and analysis that evaluates infrastructure data for accuracy, importance, and implications.
- Provide recommendations to partners and FirstNet leadership.

L.3.2.2.6.13 Continuous Diagnostic Monitoring and Mitigation

The Offeror shall provide a clear, concise description regarding its proposed approach to support continuous diagnostic monitoring and mitigation. The approach shall include but is not limited to hardware and software asset management, vulnerability management, configuration settings management, continuous network and system monitoring, and mitigation strategies.

L.3.2.2.6.14 Cybersecurity Testing and Certification

The Offeror shall provide a clear, concise description about its proposed approach to cybersecurity testing and certification. The Offeror shall describe how it will:

- Establish processes to verify security approaches through a life-cycle of selection, procurement, integration, and operations support. The testing methods shall include assessment, testing, examination, and interviewing. All testing results shall be retained to provide baseline standards for ongoing testing to ensure optimal accuracy and reproducibility.
- Validate individual systems
- Test integrated configurations
- Test independent applications and services, including the following:
 - New applications at the national level
 - User-developed or state-developed applications
 - Upgrades to approved applications
 - Security patches to approved and fielded applications

L.3.2.2.6.15 Network and Configuration Management

The Offeror shall describe how it will conduct tracking, planning, development, and implementation of new computer network defense/cybersecurity capabilities into all NPSBN systems. The Offeror shall provide documented methods, techniques, and processes to ensure that the configuration of device level, network, applications, and related components are known and changes are captured prior to implementation.

The Offeror shall provide a clear, concise description of procedures to address the following areas:

- Network management
 - Configuration management
 - Configuration identification
 - Configuration control
 - Configuration status and accounting
 - Configuration verification and audit
- Vulnerability management
- Patch management
- Centralized security log management
- Security information and event management

L.3.2.2.6.16 Environmental and Physical Security

The Offeror shall provide a clear, concise description regarding its proposed approach to environmental and physical security. The Offeror shall address, at a minimum, the following elements: power failure, humidity detection, cabinet door alarms, uninterruptable power supply power failure, access control to and within a facility, monitoring and recording of activity within a facility to include egress/ingress, movement activity within a facility after hours or in restricted areas, HVAC failure or degradation, building door alarms, generator failure, low generator fuel, low battery, closed caption television (CCTV) video surveillance systems, fire/smoke detection sensors, and protection from natural disasters (e.g., lightning/surge protection, water leak detection).

L.3.2.2.6.17 Information Security and Data Sensitivity

The Offeror shall provide a clear, concise description about its proposed approach to information security and data sensitivity. The Offeror shall, at a minimum, describe how it will:

- Encrypt and/or handle all data in transit, stored, or accessed across NPSBN environments as restricted data.
- Limit the use, dissemination, and access of restricted data to specific agencies, individuals, and situations.
- Establish mandated sensitivity and protection levels to data repositories used by FirstNet users.
- Ensure data retention follows existing record retention policies as specified by the respective data or system owner. Upon expiration of the retention period, data shall be destroyed or otherwise disposed of per agency policy.
- Prevent the release of data housed in the NPSBN to any external parties without compliance with applicable law.

L.3.2.2.7 Test Strategy

FirstNet expects to use the FirstNet Test Lab (FNTL) to test, verify, and validate features unique to public safety, as well as other devices and/or applications that may be critical to public safety, prior to their deployment into the operational NPSBN. Features unique to public safety include but are not limited to QoS, priority, preemption, and Mission-Critical Push-to-Talk. In addition to verification and validation, the FNTL will be used as a demonstration platform for NPSBN capabilities, training, and—in some cases—isolated troubleshooting of field issues. The FNTL will also be available for troubleshooting of these features should this be helpful.

The Offeror shall describe its proposed approach for providing Contractor-furnished equipment for the FNTL that will be utilized during acceptance testing for each IOC as well as any other testing FirstNet deems necessary and/or appropriate. The Offeror shall complete Table 1, Contractor-Furnished Equipment, included in Section J, Attachment J-15, noting the equipment that will be required to execute testing of features unique to public safety. This equipment is to be supplied by the Contractor.

The Offeror shall complete the Test Strategy Template included in Section J, Attachment J-12, describing its proposed approach to verifying and validating the products, features, and functions that support the NPSBN. The Offeror shall note those functions that are to be tested prior to IOC and FOC acceptance, as well as where these tests are to take place using Section C, SOO; Section J, Attachment J-3, FCC TAB RMTR; and Section J, Attachment J-8, IOC/FOC Target Timeline as references. Some features may be tested in an operational, deployed network, while others may be tested in a lab environment.

L.3.3 Volume III – Pricing

There is no page limitation for this volume. The Excel spreadsheet shall be submitted to reflect the information as stated herein and as contained in the Pricing Template (Section J, Attachment J-13). Each text page shall use Times New Roman Font Size 12, single spaced, double-sided, 8.5" x 11" (no exceptions allowed).

Certified cost or pricing data are not required for this procurement. The Contractor agrees to hold the price in its proposal firm until award or as requested in any subsequent amendment.

The failure to submit any of the information requested in this RFP may lead to the rejection of your proposal without further consideration.

The Offeror shall provide a glossary of abbreviations and acronyms used with an explanation for each. Glossaries do not count against the page limitations for their respective volumes.

The pricing volume shall contain the following information and be broken down in the following sections.

L.3.3.1 General and Structural Requirements

The Offeror shall complete the Pricing Template utilizing the Microsoft Excel electronic file provided in Section J, Attachment J-13. The Offeror shall complete all cells shaded yellow. The Offeror shall not password protect the completed Pricing Template. The Pricing Template shall not contain circular references; hidden sheets, columns, rows, or cells; or links to other files.

The Offeror shall complete the Pricing Template in order to propose the payments associated with task orders described in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders.

The Offeror shall enter positive values of the payments to FirstNet as positive numbers and negative values of the payments to FirstNet as negative numbers (as detailed in Section L.3.3.2, Payments to the Contractor).

All costs or prices provided shall be rounded to the nearest dollar. All proposal amounts shall be in U.S. currency.

The Offeror shall complete the following worksheets:

- **Payments to Contractor Worksheet** – Offerors shall propose payments to the Contractor as instructed in Section L.3.3.2, Payments to the Contractor.
- **Payments to FirstNet Worksheet** – The Offeror shall propose payments to FirstNet as instructed in Section L.3.3.3, Payments to FirstNet.
- **Delayed Payments to FirstNet Worksheet** – Offerors shall propose delayed payments to FirstNet as instructed in Section L.3.3.4, Delayed Payments to FirstNet.
- **Gross FirstNet Value Worksheet** – Offerors shall propose the gross FirstNet value as instructed in Section L.3.3.5, Gross FirstNet Value.
- **State Cost Worksheet** – Offerors shall propose state- and territory-specific costs as instructed in Section L.3.3.6, State-Specific Costs.

The Offeror shall reference the following output and calculation sheets but shall not amend them:

- **FirstNet Minimum Payment Thresholds Worksheet** – This worksheet shows the FirstNet minimum payment thresholds as identified in Section L.3.3.7, FirstNet Minimum Payment Thresholds.
- **Net Present Value Worksheet** – This worksheet shows the net present value as identified in Section L.3.3.8, Net Present Value Assumption.
- **Compliance Checks Worksheet** – This worksheet shows compliance checks that shall be met by the Offeror's proposal.

The Offeror's gross FirstNet value and all state-specific costs may inform the National Telecommunications and Information Administration's potential grant program for any states and territories that assume responsibility for deploying, operating, and maintaining their own RAN as authorized in section 6302 of the Act.

L.3.3.2 Payments to the Contractor

In its pricing volume, the Offeror may assume payments up to the aggregate total of \$6.5 billion of budget authority. These payments to the Contractor may be made upon successful achievement, approved by FirstNet, of each IOC and FOC, for the Day 1 task orders and each state and territory RAN.

The Offeror may propose the drawdown of payments, subject to the following parameters:

- Aggregate payments to the Contractor may not exceed \$6.5 billion.
- All payments to the Contractor shall be drawn down in accordance with the Act but no later than the end of fiscal year 2027.
- Payments to the Contractor for the Day 1 task orders must not exceed the nationwide elements maximum of \$1 billion. Aggregate payments to the Contractor for each IOC/ FOC milestone on a nationwide basis must not exceed \$1.5 billion.
- Offeror should assume availability of all \$6.5 billion for purposes of its submission and ultimate evaluation, although this amount may be reduced after contract award depending on the identity and number of states that assume responsibility for deploying their own RANs.
- Offeror is to provide estimated IOC/FOC completion dates consistent with the Pricing Template (Section J, Attachment J-13) as it correlates to the Offeror's proposed solution.

L.3.3.3 Payments to FirstNet

The Offeror shall propose payments to FirstNet that will be the aggregation of positive and/or negative values that it proposes for the deployment and operation of initial FirstNet-deployed RAN states. The Offeror shall propose the values of the payments to FirstNet for each of the 56 states and territories.

The total sum of these values will be the nationwide payments to FirstNet, which must be at or above the minimum payment thresholds as set out in Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet Operational Sustainability. Note that Offerors are permitted to propose a negative value for any state or territory. Additional details regarding these payments are available in Section B, Supplies or Services and Prices/Costs, Section B.2.2, State and Territory Task Order(s) – Initial FirstNet-Deployed RAN States, and Section B.2.3, State and Territory Task Order(s) – Delayed FirstNet-Deployed RANs.

Pursuant to Section M, Evaluation Factors for Award, Section M.4.5.1, Net Present Value of Payments to FirstNet, the Net Present Value of the payments to FirstNet will serve as the basis for evaluating the pricing of the Offeror's proposal.

The payments shall adhere to the following parameters:

- For proposal preparation purposes, Offerors are to assume that year 1 of the pricing template commences on the estimated IDIQ award date (as defined in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders).
- Offerors shall provide payments to FirstNet over an assumed 25-year life of the contract consistent with the proposed levels in the Pricing Template (Section J, Attachment J-13).

- Offerors should note that the estimated IDIQ award date and task order date in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders, are included for RFP planning and proposal preparation purposes only.
- All sums in the Pricing Template (Section J, Attachment J-13) shall be rounded to the nearest dollar.
- [deleted in its entirety]
- The first payment to FirstNet will be due two weeks after the state and territory task order award date (Section G, Contract Administration Data, Section G.6.2, Payments to FirstNet), regardless of date of task order award. The first payment amount will be the proposed year 1 payment in the Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13).
- Billing in each subsequent Government fiscal year will occur two weeks prior to the start of the Government fiscal year.
- [deleted in its entirety]
- The Offeror's proposed payments are severable at the state level.

If, after receipt of proposals, the Government determines there is insufficient information available to determine price reasonableness and/or to ensure a meaningful evaluation in accordance with Section M, Evaluation Factors for Award, and none of the exceptions in FAR Part 15.403-1 apply, the Offeror may be required to submit additional cost or pricing data. Information shall be provided in accordance with FAR Part 15.403-5.

L.3.3.4 Delayed Payments to FirstNet

States and territories may initially opt to undertake responsibility for the deployment and operation of their RAN, but fail to meet statutorily required approval criteria, resulting in FirstNet deciding to take responsibility for the RAN. To accommodate these scenarios, the Government intends to include options for the Contractor to provide its proposed technical solution for those states and territories. The Government may exercise the task order(s) within 900 calendar days of the state plan delivery by FirstNet to the Governor of that respective state or territory, and this will be addressed through task orders described in Section B, Supplies or Services and Prices/Costs.

The Offeror shall propose values (positive and/or negative) of the payments to FirstNet for each of the 56 states and territories based on potential delayed FirstNet-deployed RANs.

The payments shall adhere to the following parameters:

- For proposal preparation purposes, Offerors are to assume that year 1 of the pricing template commences on the estimated IDIQ award date (as defined in Section B, Supplies or Services and Prices/Costs, Section B.2, Pricing Schedules and Task Orders).
- Offerors shall provide payments to FirstNet over an assumed 25-year life of the contract consistent with the proposed amounts in the Pricing Template (Section J, Attachment J-13).
- All sums in the Pricing Template (Section J, Attachment J-13) shall be rounded to the nearest dollar.
- First payment to FirstNet will be due two weeks after the state and territory task order award date (Section G.6.3, Delayed Payments to FirstNet). First payment amount will be the proposed year 1 payment in the Delayed Payments to FirstNet worksheet of the Pricing Template (Section J, Attachment J-13).

- Each subsequent payment will be due two weeks prior to the start of the subsequent Government fiscal year (Section G.6.3, Delayed Payments to FirstNet), and will continue until the end of the 25-year period of performance of the IDIQ contract.
- The last payment amount may be adjusted pro rata to align the Offeror's proposal with the respective Government fiscal year and the end of 25-year period of performance of the IDIQ contract.
- Due to the timing of the award of Delayed Payments to FirstNet, all Delayed Payments to FirstNet that were proposed by the offeror and are beyond the 25-year period of performance of the IDIQ contract will not be required.
- The Offeror's proposed payments are severable at the state level.

See Figure 1 Notional Contracting Process – Initial Years of IDIQ Contract, and Figure 2 Notional Contracting Process – Final Years of IDIQ Contract for further clarification of the contracting process.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

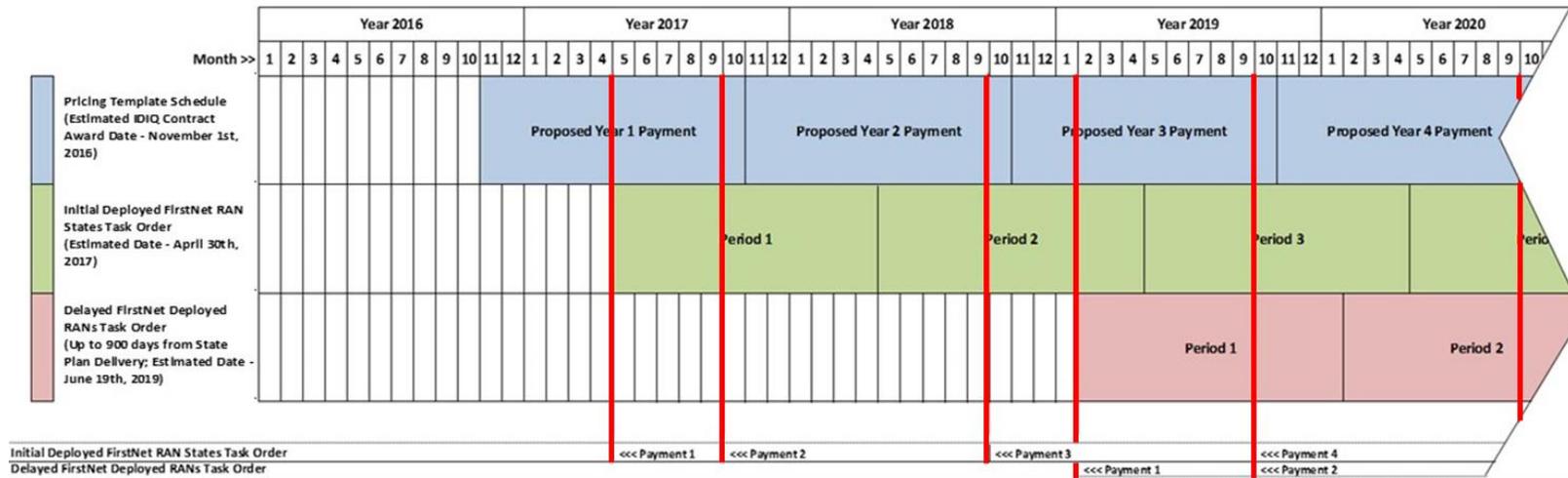


Figure 1 Notional Contracting Process – Initial Years of IDIQ Contract

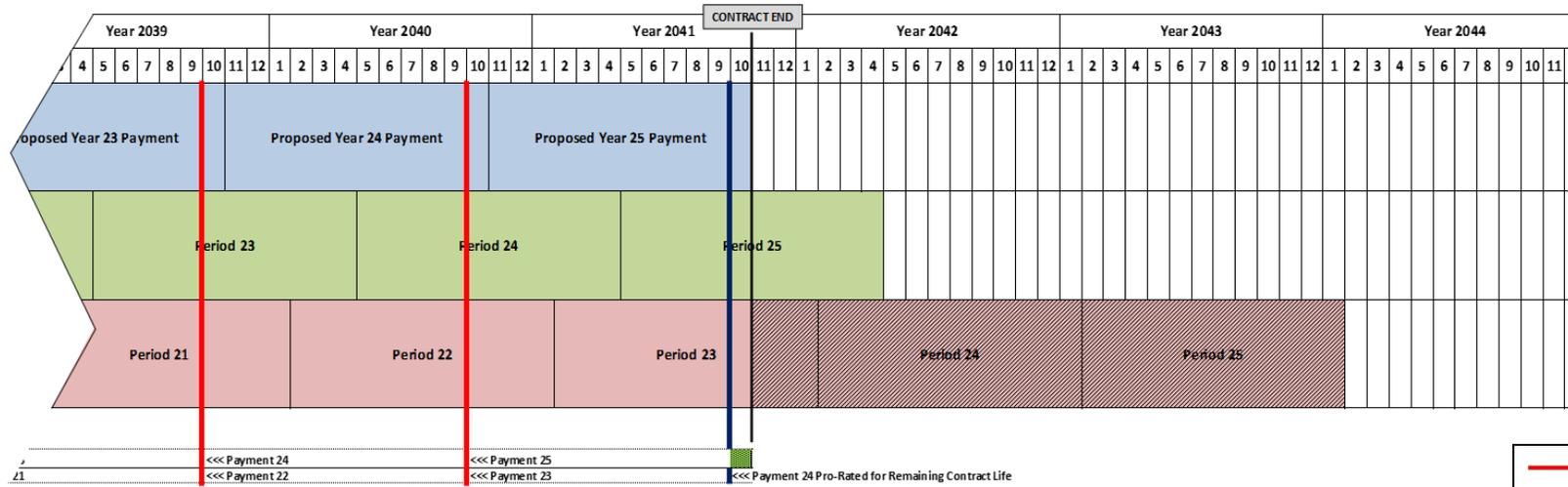


Figure 2 Notional Contracting Process – Final Years of IDIQ Contract

* Government fiscal years begin October 1st each year.

L.3.3.5 Gross FirstNet Value

The Offeror shall provide its estimated gross FirstNet value for each of the 56 states and territories. This gross FirstNet value represents all revenues (on a cash basis) that the Offeror expects to be generated by being awarded the NPSBN contract, inclusive of revenues derived from public safety use, revenues from excess network capacity, and all other revenues that the Offeror projects. Gross FirstNet value shall not include the cash identified as payments to the Contractor in Section L.3.3.2, Payments to the Contractor.

L.3.3.6 State-Specific Costs

The Offeror shall provide its estimated total projected costs (on a cash basis) incurred through the FirstNet program for each of the 56 states and territories in the appropriate worksheet in the template. These costs are defined as cash costs to deploy, maintain, and operate the state or territory's respective RAN, as well as any other state-specific cash costs, but exclude payments to FirstNet. These costs do not include any costs related to the Day 1 task orders described in Section B, Supplies or Services and Prices/Costs, Section B.2.1, Day 1 Task Orders.

L.3.3.7 FirstNet Minimum Payment Thresholds

The minimum payment thresholds represent the annual payments required for FirstNet's financial sustainability, establishing a network reserve fund, supporting recapitalization of the network, and other authorized purposes. Refer to Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet

Operational Sustainability, for the minimum payment thresholds by fiscal year. As such, the Offeror's payments to FirstNet must be at least equal to FirstNet's required minimum payment thresholds outlined in Table 1 of Section B, though the Offeror may propose payments above the minimum payment thresholds.

The proposed payments to FirstNet may differ in each Government fiscal year but must be fixed and established based on the Offeror's proposed technical solution throughout the life of the contract and in aggregate (total payments to FirstNet) must meet, and may exceed, the minimum payment thresholds in every year.

L.3.3.8 Net Present Value Assumption

Payments to FirstNet will be discounted to the present value using the 20-year Treasury bond (available at <https://www.treasury.gov/resource-center/data-chart-center/interest-rates/Pages/TextView.aspx?data=yield>) as published at 5:00 p.m. Eastern Time the day of the release of this RFP.

L.3.3.9 Re-Pricing of Payments to FirstNet and Re-Propose Solution

The Offeror shall propose payments to FirstNet no less than the minimum payment thresholds as described in Section L.3.3.7, FirstNet Minimum Payment Thresholds. Following adjustment of the payments to FirstNet—positive or negative, as applicable—to reflect states and territories that assume responsibility for deploying their own RAN, if the adjusted payments to FirstNet fall below the minimum payment thresholds described in Section B, Supplies or Services and Prices/Costs, Section B.4.4, FirstNet Operational Sustainability, the Contractor will be permitted to revise its proposal, including its payments to FirstNet.