

Name	Title	Description	QASP Reference	FirstNet Proposed Functional Owner	Respondent Proposed Functional Owner	Respondent Comment on Functional Owner	Respondent Comment on Function
FirstNet	A.0	The implementation and oversight of the Middle Class Tax Relief and Job Creation Act of 2012 created the First Responder Network Authority (FirstNet) as an independent authority within NTIA to provide emergency responders with the first nationwide, high-speed, broadband network dedicated to public safety.		N/A			
FirstNet Program Management and Governance	A.1	Terms under which the FirstNet program strategy and its various operational processes, procedures, and policies are managed. This includes management of provider(s) engagement in overall execution of FirstNet mission.		Green - FirstNet Only			
FirstNet Executive Guidance	A.1.1	FirstNet Management on the overall execution of the program and FirstNet's strategy		Green - FirstNet Only			
Strategic Direction from Board	A.1.1.1	The Board will set the strategic direction on the FirstNet program and require reviews at regular intervals to assess of progress of the program and adherence to iterative strategic milestones. The board will also facilitate the execution of the FirstNet program strategy.		Green - FirstNet Only			
Support Industry Relation Communications	A.1.2	Responsible for communications and maintaining good relations with Industries associated with Firstnet including suppliers. Responsible for internal communications of evolving market changes and needs		Green - FirstNet Only			
Conduct Outreach to Public Safety Associations	A.1.2.1	Responsible for communications and maintaining good relations with various public safety associations		Green - FirstNet Only			
Conduct Outreach to US Industry Associations	A.1.2.2	Responsible for communications and maintaining good relations with various industry associations		Green - FirstNet Only			
Standards Participation	A.1.2.3	Responsible for attending and pushing features and capabilities required by public safety in the necessary standards organizations.		Green - FirstNet Only			
International Standards Strategy Development	A.1.2.4	Responsible for developing an international strategy to collaborate and align with other countries pursuing LTE for public safety in the standards and industry organizations.		Green - FirstNet Only			
Commercial Industry Communications	A.1.2.5	This function will manage FirstNet's relationship with U.S. carriers and provider(s) to (for example) ensure FirstNet required features and functionality are represented in roadmaps and roll out schedules.		Green - FirstNet Only			
Legal Affairs	A.1.3	Responsible for ensuring compliance with the enabling act for FirstNet, and any other laws that may apply to FirstNet		Green - FirstNet Only			
Environmental Compliance Oversight	A.1.3.1	Function oversees the NPSBN compliance with environmental related laws at all times. For example NEPA.	Q-OPS-15	Green - FirstNet Only			
Spectrum Management	A.1.3.2	Responsible for supporting all FirstNet spectrum management activities including FCC and NTIA reporting requirements, 3GPP standards body interface support, and all other domestic and international standards bodies impacting FirstNet's spectrum position.		Green - FirstNet Only			
IAA Administration	A.1.3.3	Support negotiations on inter-agency agreements that may be required from time to time by FirstNet and monitor the performance of such agreements.		Green - FirstNet Only			
Regulatory Filing Review & Approvals	A.1.3.4	Review and approve all necessary regulatory filings that is necessary for the rollout of the NPSBN written by the contractors on behalf of FirstNet.		Green - FirstNet Only			
NBPSN Economic Desirability Analysis	A.1.3.5	Review and approve the economic desirability analysis done by the provider(s) for the rollout of the NPSBN.		Green - FirstNet Only			
Monitor NBPSN Legal & Regulatory Compliance	A.1.3.6	Monitor the compliance of the contractors to all rules, regulations and laws applicable to FirstNet pertaining to the rollout of the NPSBN network and services.		Green - FirstNet Only			
Technical Certification Oversight	A.1.4	Oversee the certification process and approved certifications for all equipment, applications and devices to ensure compliance with FirstNet needs and requirements		Green - FirstNet Only			
Acquisition Management	A.1.5	Responsible for identifying potential acquisitions opportunities that would directly enhance the services provided by the NPSBN for public safety. Manage the acquisition process working with the relevant technical and legal teams		Green - FirstNet Only			

Contract Administration	A.1.5.1	Responsible for the administration of all contracts which includes packaging and preparation for release, signing, and additions/addendums		Green - FirstNet Only			
Contract Life Cycle Management	A.1.5.1.1	Program management of the life cycle of all contracts including expired or contracts that require renewal, change of Scope, or transformation to a new contract		Green - FirstNet Only			
Contract Change Management	A.1.5.1.2	Responsible for the management of all changes to the contract including, redlines, agreements, addendums, and version control until final contract documents		Green - FirstNet Only			
Stakeholder Management & Marketing	A.1.6	Responsible for maintaining communications and engagement with stakeholders in the FirstNet network. This includes sharing of relevant information between stakeholders to assist in understanding of issues and the evolving needs of public safety.		Green - FirstNet Only			
Management of Opt-Out States	A.1.7	Responsible for maintaining communications and engagement with opt-out states for synchronizing on evolving network and operational compliance requirements, including solicitation of inputs on evolving public safety needs		Green - FirstNet Only			
Opt-Out States Monitoring Compliance with Laws, Regulations, Policies	A.1.7.1	Monitor the network activities in opt-out states to ensure full compliance with the laws, regulations and rules that are applicable to FirstNet		Green - FirstNet Only			
Opt Out State SMLA, Negotiations, and Life Cycle Management	A.1.7.2	Support SMLA negotiations with opt-out states. Monitor legal compliance on the performance to all SMLAs		Green - FirstNet Only			
Financial Oversight	A.1.8	Financial management of the organization which includes setting financial plans, monitoring and evaluating the implementation of these plans and ensuring that any necessary adjustments are put in place. Review the contractors' income/financial statement that measures the financial performance over a specific accounting period.		Green - FirstNet Only			
Cost Assurance	A.1.8.1	Provide analysis and reporting of current and future project costs to ascertain the overall sustainability of the program.		Green - FirstNet Only			
FirstNet Revenue Assurance	A.1.8.2	Responsible for setting up revenue assurance function for auditing and monitoring receivables, collections, and bad debt from all revenue sources		Green - FirstNet Only			
Customer Analytics	A.1.8.3	Perform analysis of data from customer behavior to help make key business decisions via market segmentation and predictive analytics.		Green - FirstNet Only			
Oversight of Secondary Use via CLA	A.1.9	This function will create and manage the framework and negotiate agreements with the contractors and other stakeholders regarding the secondary use of Band 14 via CLAs.		Green - FirstNet Only			
Compliance Auditing	A.1.10	Responsible for supporting financial, management and programmatic auditing functions to ensure compliance with all contractual terms and conditions.		Green - FirstNet Only			
Provider(s) Revenue Assurance Auditing and Monitoring	A.1.10.1	Responsible for auditing and monitoring receivables, collections, and bad debt to ensure compliance with all contractual terms and conditions from provider(s).		Green - FirstNet Only			
Process & Procedure Auditing for Services and Operations	A.1.10.2	Auditing of all services and operations processes and procedures including support of 3rd party consultants retained or working on the behalf of FirstNet, to ensure compliance with all contractual terms and conditions.		Green - FirstNet Only			
Auditing the Security of Services, Systems, Processes, and Procedures	A.1.10.3	Auditing of all security processes and procedures including support of 3rd party consultants retained or working on the behalf of FirstNet, to ensure compliance with all contractual terms and conditions.		Green - FirstNet Only			
Performance Management (QASP)	A.1.11	Responsible for oversight of auditing the provider(s) network quality assurance and performance surveillance plan (QASP) to ensure contract compliance. As the QASP will need to evolve over time, the function owner will provide input for metrics and acceptance criteria.		Green - FirstNet Only			

SLA Compliance Defining & Monitoring	A.1.11.1	Responsible for oversight of the performance of Service Level Agreements to ensure contract compliance. Develop SLA requirements as the network matures for opt-out states. Refine requirements as needed to ensure quality meets first responder needs.		Green - FirstNet Only			
KPI Defining & Monitoring	A.1.11.2	Responsible for defining and oversight of auditing NPSBN Key Performance Indicators to ensure contract compliance.		Green - FirstNet Only			
Network Monitoring	A.1.11.3	Monitoring the overall NPSBN network performance. Identifying and resolving performance issues working with the contractors.		Green - FirstNet Only			
Network Analytics	A.1.11.3.1	Performing network analytics based on performance data provided by the contractors to identify issues and trends. Work with contractors and program management on mitigation plans.		Green - FirstNet Only			
Performance Monitoring of System Engineering Lifecycle	A.1.11.4	Monitoring of the Systems Engineering Lifecycle performance within the contractors' network.		Green - FirstNet Only			
Change Management	A.1.12	Responsible for discussing and negotiating with provider(s) for changes required on technical, financial or organizational areas based on evolving needs.		Green - FirstNet Only			
Manage Organization Structure	A.1.12.1	Manage the overall program organization structure to execute the program in the most efficient manner. Responsible for discussing and negotiation with provider(s) for required organizational changes in support of Change Management		Green - FirstNet Only			
Resource Management	A.1.12.2	Responsible for discussing and negotiation with provider(s) for resource requirement changes in support of change management		Green - FirstNet Only			
Manage Change Work Orders	A.1.12.3	Responsible for discussing and negotiation with provider(s) for work order changes for the expedient execution of the program and required program changes		Green - FirstNet Only			
Definition of Network Guidelines	A.1.13	Definition of a framework for the high level network strategy and design guidelines to ensure an optimum network performance for public safety and a ubiquitous experience across all of FirstNet including provider(s), opt-out states and FirstNet.		Green - FirstNet Only			
End to End Security Polices	A.1.13.1	This function is responsible for end-to-end network security policy framework in line with evolving standards and prevailing conditions to meet FirstNet's FCC TAB and SOO end to end security requirements.		Green - FirstNet Only			
Network Identifiers Polices	A.1.13.2	This function will create the framework and policies for network identifiers to be used across all of FirstNet, FirstNet provider(s) and opt-out states to ensure nationwide public safety interoperability and interworking.		Green - FirstNet Only			
Spectrum Management & Usage	A.1.13.3	The function will create and monitor the Band 14 spectrum management framework with respect to FirstNet, FirstNet provider(s), and opt-out states.		Green - FirstNet Only			
Network Design Objectives	A.1.13.4	Definition of a framework for network design guidelines to ensure an optimum network performance for Public safety and a ubiquitous network experience across all of FirstNet including provider(s), opt-out states and FirstNet.		Green - FirstNet Only			
Roaming Administration	A.1.14	Identify and develop roaming requirements working with the contractors. Oversee the timely implementation of the roaming provider(s)hip agreements.	Q-RC-29	Green - FirstNet Only			
Use Case Development	A.1.15	Definition of all possible use cases including M2M for the NPSBN which will drive requirements for product management and network design guidelines		Green - FirstNet Only			
Public Safety Use Case Development	A.1.15.1	Definition of public safety use cases which will drive product requirements and network design guidelines		Green - FirstNet Only			
Secondary Users via CLA - Use Case Development	A.1.15.2	Definition of secondary use via CLAs use cases which will drive product requirements and network design guidelines		Green - FirstNet Only			
Others Use Case Development (including M2M)	A.1.15.3	Definition of other use cases including secondary M2M which will drive product requirements and network design guidelines		Green - FirstNet Only			
Program Management Oversight	A.1.16	Direct program management of the FirstNet program staff, both Federal and Contractor, utilizing known and accepted PM methods (PMBOK, Agile, etc.) to manage the outcomes and performance of the program.		Green - FirstNet Only			
Program/Project Impact Management	A.1.16.1	Assessment of Program impacts and identifying potential strategies or solutions to mitigate or reduce impacts to a program		Green - FirstNet Only			

Schedule Management	A.1.16.1.1	Responsible for the management of all project or program schedules. Management includes the definition, approval and assignment of the schedule within the program or project. Schedule management includes task creation, priorities, assignments, dependencies, resources, timing and slippage and critical path assessments		Green - FirstNet Only			
Risk Management	A.1.16.1.2	Assessment of Program risks and identifying potential strategies or solutions to mitigate or reduce risks to a program		Green - FirstNet Only			
Project Change Management	A.1.16.1.3	Responsible for the management of all changes to a program or project. Management includes the definition, approval and assignment of the change within the program or project. Changes range from technical to procedural, timing and resource requirements		Green - FirstNet Only			
Program/Project Communications	A.1.16.2	Responsible for the communications of all project and Program statuses. Communication includes the reporting of milestone completions, resource utilization, slippage and timing of deliverable to kept the project or program on track, including issue and roadblock resolution.		Green - FirstNet Only			
Management of Program/Project Status	A.1.16.2.1	Responsible for the reporting the status of all projects and Programs. Status management includes the reporting of milestone completions, resource utilization, slippage and timing of deliverable to kept the project or program on track, including issue and roadblock resolution.		Green - FirstNet Only			
Executive & Board Reporting	A.1.16.2.2	Responsible for the creation, delivery and presentation of an Executive Summary Report of all project information, status and completions to the Board		Green - FirstNet Only			
Sales Management Oversight and Performance Monitoring	A.1.17	Responsible for tracking the overall progress of sales and sales related activities for devices and services. Working with the provider(s) to ensure sales meet or exceed targets and if necessary agree on mitigation plans. Help define sales compensation plans	Q-DEV-1, Q-BUS-9	Green - FirstNet Only			
Life Cycle Management	A.2	Overall oversight and management of the life cycle of NPSBN services including user management, supply chain management and technical execution	Q-BUS-8	White - Comments Solicited			
User Management	A.2.1	Provide all capabilities for a state or agency to manage their customers and their users including fraud, provisioning and de-provisioning of a user and their device on the network, training for the users, and the ability for the agency to monitor performance of the local network.		White - Comments Solicited			
User Security Administration	A.2.1.1	Develop and enact processes and procedures for user security profile creation within a state or agency. Such processes and procedures should align with those of the governance body for FirstNet.		White - Comments Solicited			
User Fraud Management	A.2.1.1.1	Enacting processes and procedures to detect and prevent fraud in regard to accounts, devices, applications, and sharing of sensitive data.		White - Comments Solicited			
Customer Service Process Development	A.2.1.2	Develop and implement processes and systems for a helpdesk capability for state and agency users.	Q-BUS-1, 11	White - Comments Solicited			
Customer Service For Tier 2+ Support	A.2.1.2.1	Develop and implement higher level (Tier 2, Tier 3, and Tier 4) support capabilities to states, agencies, and users on the operation of the network, devices, and applications.	Q-BUS-11	White - Comments Solicited			
Tier 1 Troubleshooting Agency Support	A.2.1.2.2	Agencies will provide the first level of support for users in regards to how to use their devices and applications and new accessories	Q-BUS-11	Blue - Public Safety			
Provide Tier 1 type Troubleshooting Public Safety Entity support	A.2.1.2.3	Provide Tier 1 customer service/technical support to public safety users.		White - Comments Solicited			
Public Safety Entity Management	A.2.1.3	Manages user subscriptions, inventory / service fulfillment, and devices on the FirstNet system. This function allows for the capabilities of local control, device management, inventory management and device administration.	Q-APP-27	White - Comments Solicited			

Device Administration	A.2.1.3.1	Allows the agencies and FirstNet customers to manage standard, shared, and "bring your own device" devices of their users that use the FirstNet network using the device management systems. The usage of these systems will follow FirstNet, contractors, and agency policies, procedures and guidelines. The agencies are trained on how to use these capabilities through the FirstNet / contractors training programs. This function must evolve as FirstNet system requirements evolve.		White - Comments Solicited			
Hardware Management	A.2.1.3.1.1	Allows agencies to manage the HW of the device themselves including the IMEIs connected with device HW and make changes as needed. FirstNet, the contractors and device OEMs may provide and suggest guidelines for the proper HW management and changes. Maintaining proper HW devices is essential to proper and optimized device HW operation.		White - Comments Solicited			
IMEI/UICC Inventory Management	A.2.1.3.1.1.1	Manages user UICC and device associated IMEIs inventory. This function includes the ability of FirstNet device administrators, inventory specialists, and device users to conduct standard inventory process for UICCs. IMEIs are allotted per standards polices and processes which need to be followed. The GSMA provides the IMEI Allocation and Approval Guidelines Version 6.0 27th July 2011, TS.06 (DG06) which FirstNet must follow.	Q-APP-27	White - Comments Solicited			
UICC Installation on Device	A.2.1.3.1.1.2	Allows agency device administrators, inventory specialists and device users to install, swap, and remove the appropriate UICCs into the devices. Depending on the device type, its UICC may already be pre-installed by the device manufacture or during the fulfillment process, however the function of an agency being able to install UICCs directly into devices is still required.		Blue - Public Safety			
Manage, Stock, & Distribution of Hardware	A.2.1.3.1.1.3	Contractor(s) to order and return devices and device accessories through online and other systems supported by contractor(s)' device procurement process.	Q-BUS-9	White - Comments Solicited			
Policy, Apps & Content Management	A.2.1.3.1.2	Allows agencies to manage the policies, applications and content on the devices of their users. Guidelines may be provided by FirstNet, the contractors and device OEMs. Devices which do not maintain the guidelines for certain policy, applications and content may have limited access to features and functionalities.		Blue - Public Safety			
Over The Air (OTA) Management	A.2.1.3.1.3	Manages the timely configuration and updates of devices and UICCs with the necessary applications, blacklists, whitelists, security software, and network parameters. The OTA management also controls devices if they're compromised or lost.		White - Comments Solicited			
Diagnostics Monitoring & Management	A.2.1.3.1.4	Allows the agencies and customers of FirstNet to remotely capture and collect data on the devices of their users. This data would include items such as data, voice and other application usage, error reports, device configuration and similar. This information will be used by the agencies to optimize the usage of devices and their operation on the FirstNet systems.		Blue - Public Safety			
SW, OS & FW Management	A.2.1.3.1.5	Allows agencies to manage the operating systems, firmware, and software on the devices of their users. Guidelines for the proper device operating system, firmware & SW version and their updates may be provided by FirstNet, the contractors and device OEMs. Devices which do not maintain the guidelines for certain operating system, firmware and SW version may have limited access to features and functionalities.		Blue - Public Safety			
Shared Device Management	A.2.1.3.1.6	Allows agencies to manage devices and their associated accessories that are utilized by multiple users. This function manages setting and updating user profiles on the shared devices of an agency.	Q-BUS-9	Blue - Public Safety			
BYOD Management	A.2.1.3.1.7	Manages for "bring your own device" configurations for user devices from other provider(s) networks as well as on FirstNet to provide their secure operation with allowed applications.	Q-DEV-1	Blue - Public Safety			
Inventory/Service Fulfillment Management	A.2.1.3.2	Provides the agencies an ability to maintain their device and associated device accessory inventory by using the FirstNet systems. This function includes the selection, ordering, storing, and managing the end of life or replacement of devices.		Blue - Public Safety			

Manage Device Returns	A.2.1.3.2.1	The tasks associated with managing the return devices and accessories using online and other systems supported and maintained by the B/operating systems.		Blue - Public Safety			
Manage Device Ordering	A.2.1.3.2.2	The tasks associated with managing the ordering of devices and accessories using online and other systems supported and maintained by the B/operating systems.		Blue - Public Safety			
Manage Stocking of Devices	A.2.1.3.2.3	The tasks associated with managing the stock of devices and accessories.		Blue - Public Safety			
Device and Accessory Inventory Management	A.2.1.3.2.4	The tasks associated with managing the inventory of devices and accessories at agencies.		Blue - Public Safety			
Installation of In-Vehicle Devices	A.2.1.3.2.4.1	Allow agencies to manage the installation of devices and accessories into vehicles. The installations maybe be outsourced by the agencies following guidelines generated by the device manufacturers, FirstNet, contractor(s) and agencies. The installation shall also include the proper testing and certification, as required, to ensure the device and devices operate properly.		Blue - Public Safety			
Agency User Subscription Management	A.2.1.3.3	Management by the agencies of the individual user activation and deactivation process.		Blue - Public Safety			
Local Control User Provisioning & Administration	A.2.1.3.3.1	Allows agencies to input changes to the network and review reports from the network that allow them to do subscription management for their agency and/or others that work on a common incident.	Q-APP-27	Blue - Public Safety			
User Profile Life Cycle Management	A.2.1.3.3.1.1	Management by the agencies of the individual user profile, services, capabilities, and applications on the device during the user life cycle.		Blue - Public Safety			
Modification of a User Profile	A.2.1.3.3.1.1.2	Allows agencies the capability to modify a user's static profile throughout the life cycle of the profile. The profiles would be selected from a range of pre-defined list of profiles to meet the requirement for the end user.		Blue - Public Safety			
De-Provisioning of Users	A.2.1.3.3.1.2	Allows an agency to remove a user or device from the NPSBN and delete associated assignments the user had.		Blue - Public Safety			
Rating (Billing) Deactivation	A.2.1.3.3.1.2.1	Allows an agency to turn off billing for the individual user or device.		Blue - Public Safety			
User Profile De-assignment	A.2.1.3.3.1.2.2	Allows an agency to turn off the assignment of the user to a profile that remains active (for other users).		Blue - Public Safety			
Services and Applications Deactivation	A.2.1.3.3.1.2.3	Allows an agency to turn off the user or devices assignments to network services and/or device applications.		Blue - Public Safety			
Communications Groups Deactivation	A.2.1.3.3.1.2.3.1	Allows an agency to turn off the user or devices assignments to communications groups.		White - Comments Solicited			
Provisioning of Users	A.2.1.3.3.1.3	Allows an agency to provision a user or device on the NPSBN and allows it to administer profiles, services, group subscriptions for the user.		White - Comments Solicited			
User Profile Assignment	A.2.1.3.3.1.3.1	Allows an agency to assign the user to an active profile that has already been provisioned appropriately.		White - Comments Solicited			
Rating (Billing) Activation	A.2.1.3.3.1.3.2	Allows the agency to assign the appropriate billing for the individual user or device.		White - Comments Solicited			
Installation of Services & Applications	A.2.1.3.3.1.3.3	Allows an agency the ability for specific local applications to be installed on devices or specific services be activated.		White - Comments Solicited			
Communications Groups Implementation	A.2.1.3.3.1.3.3.1	Allows an agency to assign the user or devices to appropriate communications groups.		White - Comments Solicited			
Agency/State Network Monitoring	A.2.1.4	Monitoring the network operational status and the status of associated repair or reconfiguration steps in their respective area for agencies.		White - Comments Solicited			
View Agency Level Network Status	A.2.1.4.1	Monitoring network status, such as a local network operations center view for various agencies and/or states.		Blue - Public Safety			
Critical Outage Notification to Dispatch Center	A.2.1.4.2	Monitoring the status of outages and reporting that status to dispatch centers.		White - Comments Solicited			
End User Training	A.2.1.5	Support the training of users in network and device usage for the local public safety agencies and/or state jurisdictions		White - Comments Solicited			
Training on FirstNet Processes and Procedures	A.2.1.5.1	Training provider(s) in FirstNet specific processes and procedures.		Green - FirstNet Only			
Training on FirstNet Hosted Apps and Network Services	A.2.1.5.2	Training agencies on how to use FirstNet approved devices and FirstNet applications, as well as FirstNet network usage.		White - Comments Solicited			

Training Users on Agency Specific Applications and Procedures	A.2.1.5.3	Training users in the usage of agency specific applications and procedures on FirstNet.		Blue - Public Safety			
Manage Individually Liable Accounts	A.2.1.6	Provide user account services for individually liable accounts		White - Comments Solicited			
Provide Verification Services and User Provisioning	A.2.1.6.1	Provide verification and provisioning for individually liable accounts		White - Comments Solicited			
Support User Purchasing	A.2.1.6.2	Provide user purchasing processes for individually liable accounts		White - Comments Solicited			
Provide Tier 1 Support	A.2.1.6.3	Provide Tier 1 customer service/technical support for individually liable accounts		White - Comments Solicited			
Service Quality Evaluation from PS User Perspective and Improvement Activities	A.2.1.7	Contractor(s) to perform the monitoring, assessment, and improvement of public safety user experiences, utilizing both subjective and objective methodologies.		White - Comments Solicited			
Supply Chain Management	A.2.2	Manage the supplier ecosystem, life cycle management, and cost effectiveness of the NPSBN network deployment and services. This includes supplier contract negotiations and contract change management, supply chain sourcing, and supply chain performance management	Q-BUS-9	White - Comments Solicited			
Network Solutions Life Cycle Management	A.2.3	Management and oversight of all engineering activities related to the creation, evolution, and on-going operations of the NPSBN.		Green - FirstNet Only			
Technical Project Management	A.2.3.1	Oversight of the technical project management for the systems engineering activities related to the development, implementation, service delivery, technology evolution, and operations of the NPSBN.		White - Comments Solicited			
Technical Schedule & Risk Management	A.2.3.1.1	Oversight of the technical schedule and risk management for the systems engineering activities related to the development, implementation, service delivery, technology evolution, and operations of the NPSBN.		White - Comments Solicited			
Engineering & Integration Risk Management	A.2.3.1.2	Oversight of the engineering and integration risk management for the systems engineering activities related to the development, implementation, service delivery, technology evolution, and operations of the NPSBN.		White - Comments Solicited			
System Engineering Life Cycle Oversight	A.2.3.2	Oversight of the systems engineering architecture, design, and integration of the NPSBN.		Green - FirstNet Only			
Concept Development	A.2.3.2.1	Concept development of the services and technical functionalities to meet public safety marketing requirements.		Green - FirstNet Only			
Requirements Engineering	A.2.3.2.2	Product requirements collation to develop engineering guidelines and system requirements.		Green - FirstNet Only			
System Architecture Life Cycle Oversight	A.2.3.2.3	Oversight of the system architecture for each service provided by the NPSBN.		Green - FirstNet Only			
System Design and Development	A.2.3.2.4	Systems design and development of the NPSBN within the service development lifecycle.		Green - FirstNet Only			
System Integration Oversight	A.2.3.2.5	Oversight of systems integration of the NPSBN within the integration activity lifecycle.		Green - FirstNet Only			
Test and Evaluation Oversight	A.2.3.2.6	Oversight of the testing and evaluation of the NPSBN within the service lifecycle.		Green - FirstNet Only			
Transition Operation & Maintenance Oversight	A.2.3.2.7	Oversight of Transition to Operations and continuing Maintenance for the subject change of the lifecycle integration.		Green - FirstNet Only			
System Engineering Life Cycle Assessment	A.2.3.2.8	Assessment and optimization of the life cycle process for the NPSBN.		Green - FirstNet Only			
Technical Strategy	A.2.3.3	Development of long and short range roadmaps and strategy for the NPSBN.		White - Comments Solicited			
Network Solutions End-to-End Architecture Oversight	A.2.3.4	The oversight for the development of the overall end-to-end architecture of the NPSBN within each lifecycle integration.		Green - FirstNet Only			
Supply Chain Management Oversight	A.2.3.5	Oversight of all supply chain issues relating to systems engineering lifecycle activities.		White - Comments Solicited			
Technical Operations Oversight	A.2.3.6	Oversight of technical operations and practices within the contractors' network.		Green - FirstNet Only			
Oversight of Technology Implementation	A.2.3.6.1	Oversight of technology implementation operations and practices of the NPSBN.		Green - FirstNet Only			
Technology Risk Management Oversight	A.2.3.6.2	Oversight of network risk management operations and practices of the NPSBN.		Green - FirstNet Only			

Technology Change Management Oversight	A.2.3.6.3	Oversight of network change management operations and practices of the NPSBN.		Green - FirstNet Only			
Technology Configuration Management Oversight	A.2.3.6.4	Oversight of network configuration management operations and practices of the NPSBN.		Green - FirstNet Only			
Technology Refresh Oversight	A.2.3.6.5	Oversight of technology evolution planning and implementation of NPSBN.		Green - FirstNet Only			
Technical Reviews Gates	A.2.3.6.6	Management of all approval gates within the systems engineering lifecycle.		Green - FirstNet Only			
Opt-Out State Technical Compliance Oversight	A.2.3.6.7	Oversight of opt-out state compliance with FirstNet technical policy, procedure and architecture.		Green - FirstNet Only			
Engineering & Network Operations	A.3	This function represent the activities required in designing and maintaining the operation of a wireless network.	Q-RC-22	White - Comments Solicited			
Network Financial Administration	A.3.1	Management of the contractor(s)' network engineering and operations from a financial perspective. Responsible for planning the organization's long-term financial goals. Develops the organization's budget, prepares financial reports and direct investment activities. Monitor network financial performance relative to established budgets while providing reports to FirstNet.		White - Comments Solicited			
Network CAPEX/OPEX Forecasting	A.3.1.1	Function reviews expenditure trends to monitor network projects and meet approved budgets. The function also supports planning of future expenditures.		White - Comments Solicited			
Network Financial Control	A.3.1.2	Management control (as exercised in planning, performance evaluation, and coordination) of financial activities aimed at achieving desired return on investment. Direct and control all financial functions and develop analyses supporting opportunities and risk assessments. Provide information required to measure performance against budget. Prepare financial sections of strategic operating plans.		White - Comments Solicited			
Business Case Development/Analysis	A.3.1.3	Provides the management team a detailed business case analysis of the feasibility network-related services.		White - Comments Solicited			
Actual Network Spend Reporting	A.3.1.4	Produce report on variances between actual expenditures and approved spending levels, both operating and capital expense.		White - Comments Solicited			
Network Deployment	A.3.2	Network deployment represents the services and functions required to initially enable, and to continually manage growth and expansion of PSBN network services and functionality.		White - Comments Solicited			
Installation of Network Elements	A.3.2.1	Physical installation of all network equipment for operating the NPSBN, including but not limited to logistics and any necessary coordination for compliance of laws and regulations.		White - Comments Solicited			
Transmission Network Installation	A.3.2.2	End-to-end transport connectivity of each network element and verification of circuit capacity and performance (per associated acceptance tests and verification punch lists).		White - Comments Solicited			
Site Acquisition Secure & Preparation	A.3.2.3	Acquire the physical locations needed to house and deploy network elements (including RAN, core, and other assets required to deliver PSBN service). Ensure site security standards and protocols are implemented and observed throughout preparation and installation of all network elements.		White - Comments Solicited			
Warehousing/Inventory (Fixed Asset Management)	A.3.2.4	Administration of warehousing facilities and a fixed asset management inventory system to track key network element characteristics including asset status, installation history, type, model, location and associated equipment inventories. The fixed asset management system (and supporting personnel) must support financial reporting requirements as defined by FirstNet.		White - Comments Solicited			
Priority & QoS Administration	A.3.3	The administration of all priority and QoS policy frameworks for the NPSBN.	Q-RC-2	White - Comments Solicited			
Profile Configuration Setup	A.3.3.1	Setup and configure parameters of user QoS and priority profiles for different services and applications in the NPSBN.	Q-RC-2	White - Comments Solicited			
Implement Profile Changes	A.3.3.2	During an incident and periods of heavy NPSBN congestion, the priority and QoS configured in the default QoS profiles needed to be updated to allow emergency responders to have priority to obtain the communication services and resources to save lives.	Q-RC-2	White - Comments Solicited			

Drive Supplier Roadmap for QPP	A.3.3.3	Not all functions that are needed to enforce the priority and QoS settings have been implemented. The FirstNet organization and its provider(s) need to influence the equipment suppliers' roadmap in order to meet our QPP requirements.	Q-RC-2	White - Comments Solicited			
Engineering & Planning	A.3.4	Function serves planning to evolve the network elements, features, and services to meet future needs of First Responders.	Q-RC-22	White - Comments Solicited			
Long Term Feature Planning	A.3.4.1	Planning of all new features and functions beginning with feature feasibility analysis and proof of concept testing to driving suppliers' roadmap and feature product management.		White - Comments Solicited			
Proof of Concept & Field Testing	A.3.4.1.1	The proof of concept and field testing function encompasses research, prototype testing and field trials of new technology, services, features and devices to determine feasibility of deployment and interworking within the existing FirstNet network to meet new customer demand.		White - Comments Solicited			
Research/Prototype Testing	A.3.4.1.1.1	Researching and prototyping new technology, services and features to determine the viability for deployment within FirstNet to meet the needs of public safety users.		White - Comments Solicited			
Interworking Proof of Concept & Field Trials	A.3.4.1.1.2	Prototype interworking and field trials of new devices, technologies, services and features within the current FirstNet infrastructure.		White - Comments Solicited			
Prototype Device Testing	A.3.4.1.1.3	Testing new prototype devices and determine potential uses and functional value for implementation within FirstNet.		White - Comments Solicited			
Prototype RAN Feature Testing	A.3.4.1.1.4	Feature testing of new prototype RAN technology, features and functionality. This will ensure staying in sync with industry developments and standards and their applicability to the public safety marketplace.		White - Comments Solicited			
Prototype Services Testing	A.3.4.1.1.5	Testing of future prototype services enabled by existing or new technology, features and functionality. This will ensure staying in sync with industry developments and standards and their applicability to the public safety marketplace.		White - Comments Solicited			
Long Term Product Management	A.3.4.1.2	Develop three year+ public safety product roadmap to drive industry and standards development.		White - Comments Solicited			
Customer Feedback for Long Term Services	A.3.4.1.2.1	Customer feedback and requirements gathering for development of three year+ and beyond public safety product roadmap.	Q-BUS-1	White - Comments Solicited			
Feature & Services Roadmap Development	A.3.4.1.2.2	Develop systems features and services roadmap in support of the long term product roadmap		Green - FirstNet Only			
Integration of Long term NSPBN Roadmap	A.3.4.1.2.2.1	Develop roadmap to integrate long term products into the NPSBN		Green - FirstNet Only			
Standards Roadmap Development for Public Safety	A.3.4.1.2.2.2	Driving Standards organizations to implement the FirstNet long term roadmap		Green - FirstNet Only			
Long Term Feature Feasibility Analysis	A.3.4.1.3	Proof of Concept Analysis provides feasibility analysis for feature planning. This function will assess the financial and technical feasibility of the new offered or required feature or function for FirstNet.		White - Comments Solicited			
Supplier Roadmap Coordination	A.3.4.1.4	This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.		White - Comments Solicited			
Network Design & Architecture	A.3.4.2	Design and architect a cost effective and optimal NPSBN.		White - Comments Solicited			
Local Control User Administration Architecture	A.3.4.2.1	Provides the local control architecture including user/group profiles and device profiles.		Green - FirstNet Only			
Local Control User Service Admin Development & Maintenance	A.3.4.2.1.1	Maintains the local agency user/group profile, device profile, and manages the operational the services. The contractor(s) also work with agencies in providing support of any access, operational issue of the local control portal and its administration issues.		White - Comments Solicited			
Development of Local Control User Operations Guideline	A.3.4.2.1.2	Develops guideline to support network monitoring, provisioning, QPP provisioning, and accounting.		White - Comments Solicited			
Operations Guideline for Static & Dynamic Profiles	A.3.4.2.1.2.1	Develop and manage the operational guideline for static and dynamic profiles implementation, management and change control within the local agency to support their implementation of user's roles under QPP and its priority.		White - Comments Solicited			
Operations Guideline for NIMS ICS	A.3.4.2.1.2.2	The contractor(s) shall follow and implement the policy, governance guidelines of national incident management with FirstNet and other federal/local agencies.	Q-RC-13	White - Comments Solicited			

NIMS ICS Type 3,4 & 5 Local Control Process	A.3.4.2.1.2.2.1	Manage the adoption and ongoing compliance of existing NIMS ICS Types 3,4,5 protocols and processes within the local control capabilities in the NPSBN.	Q-RC-13	White - Comments Solicited			
NIMS ICS Type 1 & 2 Local Control Process	A.3.4.2.1.2.2.2	Manage the adoption and ongoing compliance of existing NIMS ICS Types 1 & 2 protocols and processes within the local control capabilities in the NPSBN.		White - Comments Solicited			
Product Development & Engineering	A.3.4.2.2	Develop and plan the network and radio products required to provide emergency responders and other public safety users communication services in the NPSBN		Green - FirstNet Only			
Mission Critical PTT (3GPP) Engineering	A.3.4.2.2.1	Engineer and design mission critical push to talk services as defined by product management.	Q-RC-9	White - Comments Solicited			
Group Communications Engineering	A.3.4.2.2.2	Engineer and design group communications services as defined by product management. This method of communications provides communications from one-to-many members of a group and is of vital importance to the public safety community. The user may manually control his/her participation in a talk group by selecting a specific talk group of interest. Talk group membership may also be infrastructure driven where existing talk groups are patched together to form a new group.	Q-RC-9	White - Comments Solicited			
Location Platform Engineering	A.3.4.2.2.4	Plan, design and engineer Location technology solutions for the NPSBN to enable true location awareness for public safety users and devices.		White - Comments Solicited			
IMS Platform Engineering	A.3.4.2.2.5	Plan, architect, design and engineer the IP Multimedia Subsystem (IMS), to support the delivery of IP multimedia services such as VoLTE, Identify Management etc..		White - Comments Solicited			
VoLTE Engineering & Design	A.3.4.2.2.5.1	Plan and design Voice over LTE service. VoLTE, Voice over LTE is an IMS-based specification. Adopting this approach, it enables the system to be integrated with the suite of applications that will become available on LTE.		White - Comments Solicited			
Other IMS Services Engineering & Design	A.3.4.2.2.5.2	Plan, design and engineer other multi-media based services on the IMS platform in support of new requirements for the public safety services, features and functions that best fit in the IMS environment.		White - Comments Solicited			
Presence Engineering & Design	A.3.4.2.2.5.3	Plan and design Presence Service. Presence service is a network service in the NPSBN which accepts, stores and distributes presence information. Presence service may be implemented as direct communication among devices.		White - Comments Solicited			
IP Messaging Engineering & Design	A.3.4.2.2.5.4	Plan and design IP Messaging. This function delivers smart and secure messaging seamlessly over IMS on communication devices. Designed specifically for mobile operators, this feature intelligently and seamlessly handles text, voice, data, and multimedia messages via public safety devices. It also pushes notifications or rich communication services over mobiles.		White - Comments Solicited			
Broadcast Platform Engineering	A.3.4.2.2.6	Plan Broadcast and Multicast Platforms required to support eMBMS services. eMBMS is a point-to-multipoint interface specification for 3GPP LTE cellular networks. The feature is designed to provide efficient delivery of broadcast and multicast services, both within a cell as well as within the core network. For broadcast transmission across multiple cells, it defines transmission via single-frequency network configurations. Target public safety applications include file delivery and emergency alerts.		White - Comments Solicited			
Designing and Engineering Mobile Device Management Systems	A.3.4.2.2.7	Plan, architect, design and engineer the device management system and network control platform(s) to support device management services to be supported on the NPSBN. The device management service is expected to support a hierarchical configuration with certain levels of control at the national network level and other levels of policy definition and control at the local PSEN.		White - Comments Solicited			
Designing and Engineering Support for Multi-Tenant Management	A.3.4.2.2.7.1	Plan and design a device management architecture which supports multi-tenant control functionality. The multi-tenant support is the ability of multiple device managers to have simultaneous access for device management control.		White - Comments Solicited			

Designing and Engineering Support for Policy & Content Management	A.3.4.2.2.7.2	Plan and design the device management features required to support policy (e.g., security requirements, forced PIN locking, etc.) and content management (e.g., application loading, browser limitations, etc.) related updates to mobile devices.		White - Comments Solicited			
Designing and Engineering Support for Over The Air (OTA) Updates	A.3.4.2.2.7.3	Plan and design the device management functions required to support sending OTA updates to mobile devices that attach to the FirstNet network, including containers necessary for "bring your own device" security.		White - Comments Solicited			
Designing and Engineering Mobile Diagnostics, Polling, & Reporting Tools	A.3.4.2.2.7.4	Plan and design the device management features required to support polling for diagnostic (e.g., device problems) and reporting measures (e.g., network performance measures) from FirstNet mobile devices.		White - Comments Solicited			
Designing and Engineering Software, OS, & Firmware Management Tools and Processes	A.3.4.2.2.7.5	Development, planning and architecture for providing operating system, SW and firmware management. This includes the capability of polling and updating all devices in the FirstNet device portfolio and connected to the FirstNet system by OTA, tethered or by roaming means including Wi-Fi connectivity to have its operating system, SW & firmware version determined, updated and verified as needed. This includes pushing notification of needed operating system, SW & firmware updates to users and allowing them to update the device or force updates.		White - Comments Solicited			
Designing and Engineering Support for Tethered Device Updates	A.3.4.2.2.7.6	Plan and design the device management functions required to support tethered updates to devices that attach to the FirstNet system, including "bring your own device".		White - Comments Solicited			
Designing and Engineering Configuration Management Tools and Systems	A.3.4.2.2.7.7	Develop, plan, architect and design device configuration management. This includes the capability of polling & updating all devices in the FirstNet device portfolio.		White - Comments Solicited			
Designing and Engineering Enabling Tools and Methods for BYOD Users	A.3.4.2.2.7.8	Plan and design the device management functions required to support "bring your own device" configurations for devices on other provider(s) networks as well as on FirstNet.		White - Comments Solicited			
Designing and Engineering for UICC/SIM Management	A.3.4.2.2.7.9	Plan and design UICC profiles for network configurations, roaming provider(s) and other necessary applications.		White - Comments Solicited			
Designing and Engineering Systems for Mobility Management	A.3.4.2.2.7.10	Plan and design the device management functionality required to support sending of mobility management related updates to mobile devices.		White - Comments Solicited			
ProSe Engineering & Design	A.3.4.2.2.8	Plan and design proximity services using LTE technologies to connect mobiles for direct communications.	Q-RC-13	White - Comments Solicited			
Direct Mode Communications Engineering	A.3.4.2.2.8.1	Plan and design the communication features of ProSe. This service utilizes location-based geofencing and beacons technologies. It needs to meet public safety QoS and reliability requirements, extend to reasonable proximity levels (up to 1 km), and provide high security and privacy level.	Q-RC-13	White - Comments Solicited			
Discovery Systems Engineering	A.3.4.2.2.8.2	Plan and design the discovery feature of ProSe. Signal discovery and situation awareness are important function of ProSe. The system needs to discover relevant signals and filter against relevant users. This will make a public safety device aware of the existence and locations of other public safety devices.	Q-RC-13	White - Comments Solicited			
Transmission Systems Management	A.3.4.2.3	Manages the backhaul links throughout the First Responder network. Ensuring the proper forecasting, ordering, and design of those links are addressed to optimally operate the network and meet the demands of users.	Q-RC-21	White - Comments Solicited			
Transmission Systems Ordering	A.3.4.2.3.1	Ordering of each site-core and core-core backhaul and backbone layer 1, 2, and 3 connections for new network elements such as cell sites or data centers or increasing connection capacity for existing network elements. Manage request timelines to support network turn-up within expected completion intervals from ordered backhaul links.	Q-RC-21	White - Comments Solicited			
Transmission Systems Forecasting	A.3.4.2.3.2	Forecasting of each site-core and core-core backhaul and backbone layer 1, 2, and 3 connections bandwidth needs based on previous and current utilization trends with input from sales on potential increase or decrease user base. Formulated forecasting plans are monitored and adjusted based on actual usage. Plans made available for operations and ordering functions.	Q-RC-21	White - Comments Solicited			

Transmission Systems Design	A.3.4.2.3.3	Design of each site-core and core-core backhaul and backbone layer 1, 2, and 3 connections for each network element based on required bandwidth and path. All forms of backhaul consisting of microwave, satellite, fiber, etc. will need to be designed optimally as required for minimal impact to the network and maximize user experience.	Q-RC-21	White - Comments Solicited			
Core Network Design	A.3.4.2.4	Design and engineer the core network for supporting the NPSBN. The core network consists of all nodes required for the proper functioning of the LTE core such as HSS, PCRF, public safety GW, MME, Routers, switches, firewalls etc.		White - Comments Solicited			
Core Architecture Design	A.3.4.2.4.1	Design the core network architecture. Architecture should be based on SAE. The core network consists of all nodes required for the proper functioning of the LTE core such as HSS, PCRF, public safety GW, MME, Routers, switches, firewalls etc.		White - Comments Solicited			
Capacity Planning	A.3.4.2.4.2	Dimension the capacity of EPC equipment required to support the expected traffic load. The process will require a capacity model or a tool to dimension the core network, i.e., to evaluate the number of nodes are required to handle the user traffic.		White - Comments Solicited			
Core Software License Management	A.3.4.2.4.3	Manage all core software licenses for all EPC equipment as well all other core peripheral equipment		White - Comments Solicited			
Traffic Management	A.3.4.2.5	Manages all transmission and subsystem traffic throughout the First Responder network. Ensuring the proper forecasting, ordering, and design of links and subsystems components are addressed to optimally operate the network and meet the demands of users.	Q-RC-19,Q-RC-21	White - Comments Solicited			
Traffic Monitoring & Reporting	A.3.4.2.5.1	Oversee network data usage from all user and subsystem generated traffic. Alerting operation teams of data transmit blocking due to capacity related bottlenecks. Providing traffic usage reports to management, forecasting, and capacity planning teams.	Q-RC-21	White - Comments Solicited			
Traffic Forecasting	A.3.4.2.5.2	Forecast air interface bandwidth data requirements for each cell site based on previous and current utilization trends with input from sales on potential increase or decrease user base. This information will drive other transmission and system traffic forecasts to adequately handle all Uplink and downlink traffic. Formulated forecasting plans are monitored and adjusted based on actual usage. Plans made available for operations and capacity planning functions.	Q-RC-19, 21	White - Comments Solicited			
Radio Network Design	A.3.4.2.6	Provides eNodeB planning to address coverage and capacity requirements. Creating solutions based on available hardware/software options with optimal location for sites and antennas.	Q-RC-22	White - Comments Solicited			
RAN License Management	A.3.4.2.6.1	Ensure the appropriate license resources are made applied at each eNodeB based on utilization and availability. Licenses should be moved from underutilized sites or acquire new licenses when all capacity management options have been exhausted.		White - Comments Solicited			
RAN Coverage Engineering	A.3.4.2.6.2	Perform the coverage design based on both indoor and outdoor performance requirements utilizing a coverage prediction planning tool. In addition taking input from optimization and capacity functions to address coverage holes or improve customer experience in over utilized areas. Solutions are developed and executed with deployment functions.		White - Comments Solicited			
Deployables Engineering	A.3.4.2.6.3	Design and station deployable resources at optimal locations throughout the regional/national areas of the network to anticipate the need for such units. Provides guidance to deployment teams on how to best integrate units into the network. Assists with the preparation of deployable designs and creates guidelines for operational use.		White - Comments Solicited			
RAN Capacity Engineering	A.3.4.2.6.4	Design capacity solutions to address sites which are overloaded to meet performance requirements from the air interface perspective.		White - Comments Solicited			
RAN Integration of Rural Carriers, Other Provider(s) networks, Opt-out States for Boundary Areas	A.3.4.2.6.5	Integrate FirstNet cell sites at the border of rural carriers, opt-out states, and other providers, thus providing seamless user handoffs between the RAN networks. In addition providing the requirements which an opt-out state will need to comply with for interoperability between the RAN networks.		White - Comments Solicited			

Application Platform Design	A.3.4.2.7	Design, implement and provide the applications platform for FirstNet. There will be collaboration with FirstNet on the capabilities that must exist in the application architecture. The application platform consists of an application store, an application development platform (for developers), and a service delivery platform to expose network services to the application layer.		White - Comments Solicited			
Mobile Application Development Platform Design	A.3.4.2.7.1	Design, implement and provide a mobile application development platform which consists of a suite of software and tools for application developers to leverage in order to develop applications for FirstNet. The tools provide the ability for application developers to stay informed of relevant development information, and also assist in ensuring applications are developed properly, efficiently and have a high success of being certified.	Q-APP-7	White - Comments Solicited			
Developer Portal Design	A.3.4.2.7.1.1	Design, implement and provide a developer portal which allows application developers to quickly get up to speed on the how to develop, test and certify applications for FirstNet. The application developer portal will provide the ability for registered users to interact with one another, discover software and services that are available for FirstNet application developers, and stay up to date on the latest news regarding FirstNet applications.	Q-APP-7	White - Comments Solicited			
Mobile Application Framework Design	A.3.4.2.7.1.2	Provide a mobile application framework that can be used by FirstNet application developers. The role of the mobile application framework is to increase the quality, innovation and time to market of the applications that are being developed for FirstNet, by providing application development tools and SDKs.	Q-APP-7	White - Comments Solicited			
Develop SDKs and Development Tools	A.3.4.2.7.1.3	Provide application relevant SDKs to help ensure innovative public safety applications can easily be developed and to ensure applications can leverage the FirstNet application, network and data APIs. SDKs include sample code, a list of APIs and API documentation. Additional development tools such as device emulators and test simulators, etc. should be provided as well. The tools and SDKs must continually be evolved and released to the development community. Additionally there must be a way for the development community to provide feedback on the application development SDKs and tools to help guide and enhance their evolution.	Q-APP-7	White - Comments Solicited			
Develop Application Test Platform	A.3.4.2.7.1.4	Design, implement and provide an environment where applications are tested and certified. The environment must support testing and certifying mobile and non mobile applications. Applications must be tested in as close to a realistic environment as possible		White - Comments Solicited			
Design App Store	A.3.4.2.7.2	Design, implement and provide the FirstNet application store. The FirstNet application store hosts applications that have been developed for use by public safety agencies. The FirstNet application store must meet the FirstNet security requirements, SLA's and local control requirements. The application store provides a way for users to discover, download, and rate applications.		White - Comments Solicited			
Design Service Delivery Platform Development	A.3.4.2.7.3	Design, implement and provide the service delivery platform which is responsible for exposing network services and data to the application layer through APIs. The network services should be accessible through the SDP in easy to use APIs that abstract the complex details from the user and provide a level of security to ensure the user does not access anything they shouldn't. The SDP consists of a North bound and South bound API's.		White - Comments Solicited			
South Facing API Implementation	A.3.4.2.7.3.1	Design, implement and provide the South Facing APIs of the service delivery platform which are responsible for connecting the SDP to the network services. This API is not exposed for application developer use, but rather is an internal API that is required to connect the SDP to the network services. The development of these APIs should align with the development and availability of new core network services and functionality.		White - Comments Solicited			

North Facing API Implementation	A.3.4.2.7.3.2	Design, implement and provide the North facing APIs that are exposed to application developers as part of a service delivery platform. The APIs provide users and applications with easy way to interact with network service or data exposed by a network service. The APIs must be clearly documented and made available to FirstNet application developers. The API must be graceful evolved with services deprecated and removed over time as minimize the impact to applications that leverage the services. Additionally the APIs must be designed and implemented to be secure and to not allow user's unauthorized access to functionality or data.		White - Comments Solicited			
System Hardening Design	A.3.4.2.8	The NPSBN must meet reliability metrics (reference SLA sections). The overall System Hardening Design includes development of the necessary costs and detailed Bill of Materials for geographic threat-based RAN and core hardening to meet availability SLAs. The awardee(s) will implement System Hardening on elements as agreed.		White - Comments Solicited			
Reliability Design	A.3.4.2.8.1	Develop both the estimate(s) of, and on-going measurements for site and system reliability. The reliability estimate will include the impact of increasing levels of hardening on which to base investment decisions.		White - Comments Solicited			
Resiliency Design	A.3.4.2.8.2	Develop equipment structures, operations plans, and organizational support structure to enable "self-healing" and mobilization for rapid return to service to meet availability as defined in SLAs.		White - Comments Solicited			
Disaster Recovery Planning/Design	A.3.4.2.8.3	Develops the mobile/deployable architecture, equipment planning (including sizing and staging locations), overall Concept of Operations (CONOPs), and organizational support structure to maintain appropriate reliability measures during disaster scenarios.		White - Comments Solicited			
Provide Cloud Services Administration	A.3.4.2.9	Design, implement and provide the FirstNet cloud services and cloud platform which provides FirstNet users (agencies, application developers, etc.) with cloud secure cloud services comparable to what are provided by commercial cloud providers (e.g. IaaS, PaaS, SaaS). The FirstNet cloud must ensure that the SLAs that are in place for users and software deployed to the cloud are met. The administration interface must include the ability to monitor the health and status of the cloud software/service and receive notifications when the health degrades. Additionally the cloud platform must provide the software tools necessary to report issues and manage cloud resources.		White - Comments Solicited			
Develop and Manage Agency Information Homepage	A.3.4.2.9.1	Design, implement and provide the customizable agency information homepage which is used to provide information to public safety users about their local agency. The information can include agency alerts, information about incidents that are in progress, etc. The status web page should be made available to public safety agencies as Software as a Service that each individual agency can manage and tailor in a manner that will best suite their needs.		White - Comments Solicited			
Develop and Manage Application Hosting	A.3.4.2.9.2	Design, implement and provide hosting for applications, software and services that may be developed by Agencies or 3rd party application developers. The applications, platform and software must be able to be easy to manage through the hosting tools. Applications will have different requirements, including user load, security, auditing, etc. and the application producers must be able to tune their software and the infrastructure in order to meet the needs of the users. Tools and services to assist in the management of 3rd applications must be available as part of the FirstNet cloud offering.		White - Comments Solicited			
Develop and Manage Cloud Services	A.3.4.2.9.3	Design, implement and provide the suite of services that will be made available through the FirstNet cloud platform. The FirstNet cloud will provide 'X'as a Service (Software, Infrastructure, Platform, etc.) capabilities to agencies and FirstNet application developers. The FirstNet cloud services must meet the FirstNet security requirements, and meet the FirstNet SLA's.		White - Comments Solicited			

Develop BigData Analytic Platform and Associated Services	A.3.4.2.9.4	Design, implement, and provide a BigData and analytic platform that can be leveraged by agencies and application developers. The analytics should include predictive, prescriptive, descriptive, diagnostic, etc. analytics, as well as new cutting edge analytic methods.		White - Comments Solicited			
End to End NPSBN Architecture Definition	A.3.4.3	Design the end to end network architecture of a NPSBN. The end-to-end network architecture, is the logical and structural layout of the network, consisting of transmission equipment, software and communication protocols and infrastructure (wired or wireless) transmission of data and connectivity between components from the user to the end point of the NPSBN.	Q-RC-19, 21	White - Comments Solicited			
Business Support Systems (BSS) Management	A.3.5	Administrative services generating the various defined business support, billing, and business intelligence (BI) services, and all the systems necessary to maintain the defined BSS services. The BSS includes the planning and development of an architecture to meet FirstNet primary and secondary usage records, billing records, customer retention management, service and device usage and performance information, and other BI functions.		White - Comments Solicited			
Local Control: Service & User Provisioning	A.3.5.1	Perform administration of service and user provisioning as defined in the provisioning reference function. The administration services include the functions of adding, changing, and deleting of services, devices, applications, user profiles, QPP settings, and other such provisioning services for PSEs, other primary, and secondary users. Local control capability includes ability to manage all user and service-defined functions at the public safety Entity level including multi-tenant capabilities to ensure confidentiality, control, and management within each PSE.		White - Comments Solicited			
Billing Administration	A.3.5.2	Administration of user, usage, and all other account billing, charging, invoicing, and/or revenue-generating activity. Included in this function are the internal capabilities to enable billing administrators to generate, receive, and monitor primary and secondary user billings.		White - Comments Solicited			
Billing Reporting	A.3.5.2.1	Provides the scheduled and unscheduled reports on billing, invoicing and other account services. Scheduled reports include detailed usage, charging, and other accounting on a user, device, application, and services as defined by the rating and charging structures. Billing Reporting defines both internal reports and reports generated for end users.		White - Comments Solicited			
Usage Reporting	A.3.5.2.1.1	Defines the usage reporting required for all accounts, users, and usage types. PSEs will require standard reports in support of billing verification, and user, device, and service management.		White - Comments Solicited			
Billing Data Analytics	A.3.5.2.1.2	Defines the reporting and analytics services provided to FirstNet and/or PSEs including processing, analytics, data and process mining, business performance management, benchmarking, and/or predictive analytics on users, usage, services, applications, security and other user functions.		White - Comments Solicited			
Revenue Assurance (Fraud Management)	A.3.5.2.2	Provide for revenue assurance through reports, auditing, and other validation processes to ensure accuracy of charged and collected revenue and costs. The function includes the auditing of BOTH the incoming (from primary secondary users/usage, etc.) and outgoing revenues (roaming, backhaul, transport expenses, etc.).		White - Comments Solicited			
Roaming Billing Administration	A.3.5.2.3	Provides systems capability and services to administer user and/or usage billing for primary and secondary users with roaming provider(s). Maintain detailed records of CDRs and other billing records for historical review.		White - Comments Solicited			
Opt Out State Billing Administration	A.3.5.2.4	Provide systems capability and services to administer user billing for primary and secondary users in opt-out states. Maintain detailed records of CDRs and other billing records for historical review.		White - Comments Solicited			
Secondary Usage via CLA Billing Administration	A.3.5.2.5	Provide systems capability and services to administer user billing for secondary users. Maintain detailed records of CDRs and other billing records for historical review.		White - Comments Solicited			

Invoicing & Billing	A.3.5.2.6	Creation, delivery, processing, and collection of invoices or bills for any services rendered by FirstNet to primary, secondary, opt-out, and/or provider(s). The services include the processing of associated data records from those provider(s) to generate accurate bills and invoices.		White - Comments Solicited			
Rating & Pricing	A.3.5.2.7	Defines the services to develop and update user, usage, and service pricing for FirstNet primary, secondary, and provider(s) services. Included are the services to implement and verify accurate implementation of rating and pricing to users.		White - Comments Solicited			
Business Intelligence	A.3.5.3	Defines the overall services to provide business intelligence capabilities to FirstNet and PSEs. Included are the systems and reporting to support analytical processing, analytics, data and process mining, business performance management, benchmarking, predictive analytics, and other analyses in support of business intelligence.		White - Comments Solicited			
User Business Intelligence Data Analytics	A.3.5.3.1	Provide systems and remote desktop user interfaces to support "self-service" analyses by FirstNet and/or PSEs to provide analytical processing, analytics, data and process mining, business performance management, benchmarking, and/or predictive analytics on users, usage, services, applications, security and other user functions.		White - Comments Solicited			
Billing Systems Maintenance	A.3.5.4	Ensure all billing software and hardware systems are maintained to the appropriate level to ensure the provisioning and operation of all the required billing functions necessary to run the NPSBN billing operations error free. Functions include generating, receiving and monitoring primary and secondary user billings.		White - Comments Solicited			
Define Billing Profiles	A.3.5.4.1	Define standard and custom user, service, application, and device profiles for use in rate plans and other billing administration services.		White - Comments Solicited			
Mediation Platform Administration	A.3.5.4.2	Develops, administers, and maintains mediation platforms between core and billing system elements in support of interfaces to FirstNet, provider(s), opt-out states, and/or other third-parties.		White - Comments Solicited			
Billing Software Updates	A.3.5.4.3	Ensures the systems for billing, mediation platforms, CRM, SEM, BI and other systems are updated and functions to fully support all features and functions provided in the FirstNet service offering. Performance during software updates must meet relevant availability SLAs.		White - Comments Solicited			
Billing System Reporting	A.3.5.4.4	Develop and maintain administration servers, remote desktop user interface and control systems for Billing Administrators to generate various reporting on billing functions.		White - Comments Solicited			
Billing Intelligence Data Analytics	A.3.5.4.4.1	Develop and maintain servers, remote desktop user interface, and control systems for "self-service" Business Intelligence capabilities to be performed by FirstNet and PSEs. Included in BI and Billing Data Analytics are analytical processing, analytics, data and process mining, business performance management, benchmarking, and/or predictive analytics on users, usage, services, applications, security and other user functions.		White - Comments Solicited			
System Usage Reporting	A.3.5.4.4.2	Develop and maintain servers, remote desktop user interface, and control systems for "self-service" Usage Reporting capabilities to be performed by FirstNet and PSEs.		White - Comments Solicited			
Customer Relationship Management (CRM)	A.3.5.5	Develop and maintain servers, remote desktop user interface, and control systems for CRM capabilities to be performed by the NPSBN and extend limited capabilities to certain public safety agencies.		White - Comments Solicited			
Data Storage Administration	A.3.5.6	Develop architecture for, and administer the ongoing operations of all user, usage, billing, CRM, performance, network and other data. Data Storage Administration to manage all required data storage. Data Storage Administration must be developed such that data availability SLAs are met.		White - Comments Solicited			
Performance Management	A.3.6	Provides the capabilities to optimize the user performance and experience of the overall NPSBN.	Q-RC-22	White - Comments Solicited			
Service Optimization	A.3.6.1	Optimize the performance of services to based on the review and analysis of relevant network performance, customer service feedback and trends.	Q-RC-22	White - Comments Solicited			

Parameter Standardization	A.3.6.2	Review and analysis of relevant network performance parameters and trends and standardize parameters or network configuration in order to improve service performance and quality and support best practice guidelines	Q-RC-22	White - Comments Solicited			
Network Optimization	A.3.6.3	Network optimization to meet QASP KPIs and network guidelines using outage mitigation, coverage tuning, capacity tuning, configuration optimization and coverage field testing and measurement.	Q-OPS- 4	White - Comments Solicited			
Outage Mitigation	A.3.6.3.1	Responsible for ensuring the network configuration is optimized to mitigate against potential single points of failure. Support efforts in all technical areas to minimize the potential possibility of outages due to common network events	Q-RC-29	White - Comments Solicited			
Coverage Tuning	A.3.6.3.2	Measure radio performance in the field using appropriate methods and optimize radio parameters to improve the quality of radio coverage.		White - Comments Solicited			
Capacity Tuning	A.3.6.3.3	Monitor network capacity in the core and radio networks and optimize network configuration to ensure sufficient network capacity for public safety is planned and implemented for the newer team in the NPSBN		White - Comments Solicited			
Configuration Optimization	A.3.6.3.4	Monitor network performance in the core and radio networks and optimize network configuration for improved performance, quality and reliability for public safety	Q-OPS- 4	White - Comments Solicited			
Coverage Field Testing & Measurement	A.3.6.3.5	Measure radio performance in the field using appropriate methods and provide test reports to various departments to review, analyze and optimize the performance of the NPSBN		White - Comments Solicited			
KPI Monitoring	A.3.6.4	Monitoring and development all necessary QASP reporting to FirstNet in compliance with contractual requirements.	Q-DEV-8	White - Comments Solicited			
O&M Interfaces & Tools	A.3.7	Provide infrastructure of overall network and user experience performance reporting. This includes the development, maintenance, storage, and formulation of all pegs and KPIs based on input from equipment provider(s) specifications or network personnel recommended definitions.		White - Comments Solicited			
Data Storage for Tools Administration	A.3.7.1	Maintaining databases containing vast amounts of network performance data with security support. Expanding storage space as needed. Troubleshooting failures or errors. Validating data integrity. Upgrading servers with latest software or firmware. Backup all of critical data.		White - Comments Solicited			
Field Measurement Tool Management	A.3.7.2	Management of air interface analysis tools utilized in the field to troubleshoot issues or measure network performance. Upgrades, repair, and tracking required on a periodic bases.		White - Comments Solicited			
Element Management System Administration	A.3.7.3	Support element management systems for upgrades and troubleshoot failures. Provide or revoke user access to such systems. Maintain database backups of network configuration.	Q-OPS-4	White - Comments Solicited			
KPI Development	A.3.7.4	Development and agreement of formulas to create Key Performance Indicators utilizing recommendations from equipment provider(s) or modifications based on input from other functional teams.		White - Comments Solicited			
KPI Reporting	A.3.7.5	Design and distribution of network performance and status reports throughout the organization. Build customized reports based on input from various functional teams.		White - Comments Solicited			
Network Events & Alerting Administration	A.3.7.5.1	Reporting of network outages or errors for alerting network engineers to address immediately. Severity levels of incident can be created based on network impact.		White - Comments Solicited			
Network Management	A.3.8	The network management function supports the major operational related items for maintaining network performance. Ensuring all elements of the network are functioning appropriately.		White - Comments Solicited			
Operations & Maintenance	A.3.8.2	Performing all aspects related to efficient operations of the NPSBN, including all ITIL functions around service support and on-going service delivery.		White - Comments Solicited			

Experience Center & Training Creation and Management	A.3.8.2.1	Create and manage the FirstNet lab functions responsible for test case creation, performance testing and training for specific public safety/FirstNet features including validating system requirements such as QPP, PTT, location, LMR/LTE interconnectivity, device range and RF performance. Additionally, the function will coordinate training; specifically dispatch operator and local agency FirstNet network feature training. Specifically, the FirstNet lab will manage: <ul style="list-style-type: none"> • Contracting including testing SOW creation • Management reporting • Program management • On site testing quality assurance and auditing • Test result evaluation • Public safety use case validation 		White - Comments Solicited			
Public Safety ICS Training	A.3.8.2.1.1	Development of network training programs to support of ICS communications staff for incident and event communication management.		White - Comments Solicited			
NPSBN feature demonstrations	A.3.8.2.1.2	Demonstrate and showcase FirstNet-specific features and functionality for FirstNet stakeholders and agencies including QPP, PTT, location, LMR/LTE interconnectivity, device range and RF performance.		White - Comments Solicited			
Implementation & Updates Management	A.3.8.2.1.3	Test new software, firmware and hardware features and updates to FirstNet prior to their deployment. This function will also insure these updates function properly between opt-out states and FirstNet and provide state and agency requirements for implementation (prior, during and after).		White - Comments Solicited			
Network Maintenance	A.3.8.2.2	Network maintenance includes planned activities including software upgrades and patch releases, translations audits, database maintenance, and end-of-life replacement programs. All network maintenance activities are tracked via the change management system/protocol.		White - Comments Solicited			
Hardware & Software Updates	A.3.8.2.2.1	Software updates (including major and point releases) will occur across multiple network elements and must be coordinated and tested to ensure all user services continue to perform as expected. (Reference "Change Management"). Regression testing and back-out procedures must be in place to validate and/or revert to prior configuration.		White - Comments Solicited			
Equipment or Service Repair	A.3.8.2.2.2	Repair includes physical (hardware or facility replacement/repair) and software/translation related modifications required to restore service to full user functionality.		White - Comments Solicited			
Equipment Spares Management	A.3.8.2.2.3	Spares management represents the process and logistics of ensuring spare parts are properly provisioned and optimally physically located to enable rapid service restoration. Spares management is closely tied to field network operations and the fixed asset management system.		White - Comments Solicited			
Preventative Maintenance	A.3.8.2.2.4	Preventative maintenance involves activities designed to maintain high levels of network performance and to prevent basic network impairments. Such maintenance includes scheduled functional testing (such as battery and generator testing), general site maintenance and scheduled cleaning, and RF path (radio, cable) quality testing and verification.		White - Comments Solicited			
Operations	A.3.8.2.3	The operations function serves to manage the configuration, optimization, and implementation of the network elements.		White - Comments Solicited			
Network Configuration Management	A.3.8.2.3.1	Manage the configuration of all NPSBN equipment for network operations to ensure design and operational compliance. All NPSBN nodes need to be configured to meet design and service requirements that meet the public safety needs.	Q-OPS-4	White - Comments Solicited			
Roaming Configuration Management	A.3.8.2.3.1.1	Manage the configuration of each NPSBN node to support and provide the designed roaming functionality and features.	Q-RC-29	White - Comments Solicited			

Network Identifier Management	A.3.8.2.3.1.2	Design and manage network identifiers. Examples are (1) PLMN, Public Land Mobile Network which consists of a Mobile Country Code and Mobile Network Code, (2) IMSI, International Mobile Station Identifier, which determine the device or user's home network and identity. Other key LTE network identifiers included but not limited to TAI, GUTI, ECGI, IMEI, IMEISV.		White - Comments Solicited			
Managing Network Settings For Mobile Devices	A.3.8.2.3.1.3	The national network level to support the device management related updates to support network related settings. Examples of network setting updates would be in the area of SIM OTA updates to support mobility management and APN settings.		White - Comments Solicited			
Lawful Intercept Management (CALEA)	A.3.8.2.3.2	CALEA's (Communication Assistance of Law Enforcement Act) purpose is to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to wiretap any telephone traffic; it has since been extended to cover broadband internet and VoIP traffic. This function is managed by the contractor(s) if there is any wiretapping to be established for any suspect in the public safety network. The contractor(s) will work with the Law Enforcement Agencies and provide the suspect(s) location, voice and other called party information.		White - Comments Solicited			
Other Services Intercept Authorization & Execution (e.g. location)	A.3.8.2.3.2.1	Manage the authorization and execution of Other services intercept with Law Enforcement Agency in providing the "suspect(s)" location (CellID, Lat, Lon) etc.		White - Comments Solicited			
Cyber Monitoring Authorization & Execution	A.3.8.2.3.2.2	Manage the authorization and execution of Cyber Monitoring with Law Enforcement Agency in providing the "suspect(s)" location, ip-address, VoIP services (OTT applications) etc.		White - Comments Solicited			
Signaling Intercept Authorization & Execution	A.3.8.2.3.2.3	Manage the authorization and execution of Signaling intercept with Law Enforcement Agency in providing the "suspect(s)" location and intercepting the signaling traffic. The suspect(s) call identifying information and Location, Tracking Area Updates are periodically sent to Law enforcement agency. The CDR report is also provided by contractor(s) to the Law Enforcement.		White - Comments Solicited			
Voice Intercept Authorization & Execution	A.3.8.2.3.2.4	Manage the authorization and execution of Voice intercept with the Law Enforcement Agency in providing the suspect(s) Voice traffic in real-time.		White - Comments Solicited			
Data Intercept Authorization & Execution	A.3.8.2.3.2.5	Manage the authorization and execution of Data intercept with the Law Enforcement Agency in providing the suspect(s) Data traffic in real-time.		White - Comments Solicited			
Messaging Intercept (SMS/MMS) Authorization & Execution	A.3.8.2.3.2.6	Manage the authorization and execution of Messaging intercept with the Law Enforcement Agency in providing the suspect(s) message (SMS, MMS) traffic in real-time. CDR's are also provided by contractor(s) to the Law Enforcement. The signaling and Bearer information of the SMS, MMS traffic of the suspect(s) is provided by contractor(s) to the Law Enforcement Agency.		White - Comments Solicited			
Release Management	A.3.8.2.3.3	Managing new software and hardware updates (minor and major releases) across the NPSBN.		White - Comments Solicited			
New or Upgrade Network Elements Release Management	A.3.8.2.3.3.1	Managing hardware updates across the NPSBN as required to support the product management roadmap, enhanced functionalities, and capacity needs.		White - Comments Solicited			
New or Upgrade Software Release Management	A.3.8.2.3.3.2	Managing software updates across the NPSBN as required to support the product management roadmap, enhanced functionalities, and capacity needs. For example major releases will be synchronized with 3GPP cycles.		White - Comments Solicited			
New or Upgrade Feature or Functionality Release Management	A.3.8.2.3.3.3	Managing feature updates across the NPSBN as required to support the product management roadmap, enhanced functionalities, and capacity needs. For example MCPTT, GCSE, and ProSe.		White - Comments Solicited			

Device Management Systems Operations	A.3.8.2.3.4	Utilize the device management system(s) to support device management services for mobile devices on the NPSBN. These operations will allocate certain levels of control at the national network level and other levels of policy definition and control at the local PSEN.	Q-RC-19	White - Comments Solicited			
Operating the Multi-Tenant Management Access and Permissions	A.3.8.2.3.4.1	Manage access system permissions for agency administrators to the device management system.		White - Comments Solicited			
Operating Device Policies & Content Management	A.3.8.2.3.4.2	Utilize the device management functionality to support policy (e.g., security requirements, forced PIN locking, etc.) and content management (e.g., application loading, browser limitations, etc.) related restrictions to mobile devices.		White - Comments Solicited			
Management of Over The Air (OTA) Updates	A.3.8.2.3.4.3	Utilize the device management features which support sending OTA updates to mobile devices that attach to the FirstNet network, including containers necessary for "bring your own device" security.		White - Comments Solicited			
Managing Tools for Diagnostics, Polling, & Reporting on the Device	A.3.8.2.3.4.4	Utilize the device management features to support polling for diagnostic (e.g., device problems) and reporting measures (e.g., network performance measures) from FirstNet mobile devices.		White - Comments Solicited			
Mobile Device Software, OS, & Firmware Management	A.3.8.2.3.4.5	Operating and maintaining the operating system, SW and firmware update capability for all devices in the FirstNet device portfolio and connected to the FirstNet system by OTA, tethered or by roaming means including Wi-Fi connectivity to have its operating system, SW & firmware version determined, updated and verified as needed. This includes allowing for new devices to be added while supporting older devices versions.		White - Comments Solicited			
Updating Mobile Device Via Tethering Arrangements	A.3.8.2.3.4.6	Utilize the device management features which support making tethered updates to devices that are attach to the FirstNet system through a tethered connection (non wireless), including "bring your own device".		White - Comments Solicited			
Operating and Maintaining Mobile Device Configuration Management	A.3.8.2.3.4.7	Operating and maintaining the device configuration update capability for all devices in the FirstNet device portfolio and connected to the FirstNet system by OTA, tethered or by roaming means including Wi-Fi connectivity to have its operating systems, software, and firmware version determined, updated and verified as needed. This includes allowing for new devices to be added while supporting older devices versions.		White - Comments Solicited			
Updating and Tracking Mobile Devices for BYOD Users	A.3.8.2.3.4.8	Utilize the device management function to set and provide updates for "bring your own device" configurations for devices from other provider(s) networks as well as on FirstNet.		White - Comments Solicited			
Providing UICC/SIM Management for Devices	A.3.8.2.3.4.9	Utilize the device management function to set and update UICC configurations and applications.		White - Comments Solicited			
Operating Mobility Management for Devices	A.3.8.2.3.4.10	Utilize the device manager to control and provide updates to devices in regards to mobility management such as roaming provider(s) and prioritization.		White - Comments Solicited			
Network Impairment Triage	A.3.8.2.3.5	Network impairment triage is the operational process by which service impairments are methodically diagnosed and the proper resources are engaged to resolve the impairment in the most expeditious manner possible. Tier 1, 2, and 3 resources are engaged as required to facilitate resolution.		White - Comments Solicited			
After Action Reporting	A.3.8.2.3.5.1	Create after action reports to be prepared after major service impairments to document the cause(s), resolution, and recommendations to avoid future similar network impairments. After action reports are incorporated into process modifications and training programs to minimize issue reoccurrence and to speed time to repair for similar or related future events.	Q-OPS-25	White - Comments Solicited			
Tier 1 Support	A.3.8.2.3.5.2	Tier 1 support is focused on network monitoring, alarming, and reporting (including resource dispatch) to resolve network impairments. Tier 1 resources resolve the majority of network impairments without requiring escalation to Tier 2 or Tier 3. Tier 1 support also coordinates higher level impairments, preparing after action reports and updating protocols to minimize future impairments.		White - Comments Solicited			

Tier 2 Support	A.3.8.2.3.5.3	Tier 2 support represents the second highest level of escalation in an impairment scenario. Support is typically provided by on-site or on-call operations subject matter expertise at the operator (vs. supplier) level.		White - Comments Solicited			
Tier 3 Support	A.3.8.2.3.5.4	As the highest level of technical escalation, Tier 3 escalations involve supplier subject matter expertise (engineering, architecture and/or operations) and operator engineering/architecture resources. Tier 3 resources are engaged as agreed to in relevant service level agreement(s).		White - Comments Solicited			
Problem Management	A.3.8.2.3.6	Problem management entails the identification of network or service fault or performance degradation and taking the steps necessary to isolate and resolve the trouble incident. This can also include establishing a temporary fix of the problem to restore service until the a permanent fix can be implemented.		White - Comments Solicited			
Problem Investigation & Resolution	A.3.8.2.3.6.1	This is the successful implementation of recommendations (patches, re-architecture, additional capacity) of post/reoccurring service degradations. Root cause of past events are completed and recommendations are successfully implemented into production.		White - Comments Solicited			
Continual Service Improvement	A.3.8.2.3.6.2	Continual service improvements are the review of recommendations and implementation across all services for applicability to reduce further risk of problem reoccurrence.		White - Comments Solicited			
Quality Assurance & Testing	A.3.8.2.4	Perform the overall testing for all devices to ensure compatibility and performance specifications are met on the network.		White - Comments Solicited			
Designing and Carrying out Mobile Device Carrier Acceptance Test Plans and Approvals	A.3.8.2.4.1	The different types of testing will be managed and conducted primarily by the device OEMs & Contractors. FirstNet and the local agencies may be included in or support the testing depending on the scope. FirstNet and local agency may have input into device testing and certification plans depending on device type, features and functions. FirstNet and the local agencies may also conduct regression or spot check testing to confirm the OEM and contractor(s)' efforts. The testing scope will include security, performance and standards body certification. The testing of the device includes the testing of it's associated planned for and potential accessories.	Q-DEV-2	White - Comments Solicited			
Device Performance Testing	A.3.8.2.4.1.3	This function specifically calls out the testing of device performance, including RF, mobility and similar quality features.	Q-DEV-5	White - Comments Solicited			
Device Interoperability Testing	A.3.8.2.4.1.3.2	Testing of features and functionality interoperating with other devices and systems.		White - Comments Solicited			
Application Interoperability Testing	A.3.8.2.4.1.3.5	Testing device application Interoperability ensuring device applications meet performance requirements.		White - Comments Solicited			
User Equipment Certification	A.3.8.2.4.1.4	Provide appropriate test suites to ensure that devices authorized and certified as FirstNet compliant work in the desired manner. Support appropriate network specific tests, such as RAN IOT and vertical features specific to FirstNet.		White - Comments Solicited			
Conduct FCC Type Certification	A.3.8.2.4.1.4.1	Work with provider(s) to verify that they run the appropriate test suites to meet FCC type acceptance requirements. Support the FCC in their definition of type acceptance requirements.		White - Comments Solicited			
Conduct PTCRB Certification	A.3.8.2.4.1.4.2	Work with provider(s) to ensure that they run the appropriate test suites to meet PTCRB requirements. Work with PTCRB to construct the appropriate test suites and get them approved for distribution to the various industry test houses.		Green - FirstNet Only			
Device Administration of Secondary User via CLA	A.3.8.2.4.1.5	Devices used by secondary users may not conform to the entire FirstNet testing suite. This function manages the types and nature of secondary user devices allowed to access the network (e.g., M2M modems).		White - Comments Solicited			
Field Testing	A.3.8.2.4.2	Function involves field testing for major software upgrades and new services prior to activating them within the FirstNet network. This function does not cover interconnection, application certification, UE nor configuration testing.	Q-OPS-4	White - Comments Solicited			
Major Software/Hardware Upgrade Testing	A.3.8.2.4.2.1	Testing of new software and hardware updates (minor and major releases) across the NPSBN.		White - Comments Solicited			

New Services Testing	A.3.8.2.4.2.2	Testing of new services key to the success of FirstNet and public safety after they have been thoroughly testing and validated. Some examples of new feature implementation under this function for FirstNet such as GCSE, eMBMS, ProSe, UE Relays, high power UEs and MCPTT (Mission Critical PTT over LTE).		White - Comments Solicited			
Interconnection Testing	A.3.8.2.4.3	Testing of interconnection services, especially those connecting between eNB and the FirstNet core for both opt-in and opt-out states. Security testing of these links may also be incorporated.	Q-RC-19, 21	White - Comments Solicited			
S1 Interconnection Testing (Opt-out RAN)	A.3.8.2.4.3.1	Testing of S1-U (User Plane) and S1-MME (control plane) interconnection services connecting between eNB and the FirstNet core for opt-out RAN. IPsec security over these links will also be tested.	Q-RC-19, 21	White - Comments Solicited			
ISP/PSTN Interconnection Testing	A.3.8.2.4.3.2	Testing between FirstNet's core network and core network services and commercial ISP and PSTNs for delivery of data and voice services between FirstNet and other providers.	Q-RC-19, 21	White - Comments Solicited			
Roaming Interconnection Testing	A.3.8.2.4.3.3	Interconnection testing between FirstNet's core network roaming IPX services to provide roaming services to FirstNet users. Roaming interconnection testing between FirstNet and other providers could involve the following interfaces: S6a, S8, and SGI for local breakout.	Q-RC-19, 21	White - Comments Solicited			
Inter-carriers Interconnection Testing	A.3.8.2.4.3.4	Interconnection testing between FirstNet's core network and core network and other wireless operators (perhaps connected directly) for delivery of data and voice services between FirstNet and other wireless providers. This testing could involve the following interfaces: S6a, S8, and local breakout.	Q-RC-19, 21	White - Comments Solicited			
WiFi Interconnection Testing	A.3.8.2.4.3.4.1	Interconnection testing via WiFi methods between FirstNet's core network and core network and other wireless operators for delivery of data and voice services between FirstNet and other wireless providers.	Q-RC-19, 21	White - Comments Solicited			
Backhaul & Backbone Interconnection Testing	A.3.8.2.4.3.5	Testing microwave, fiber, satellite and cable systems layers 1, 2, and 3 including all failover links related to cell site-core and core-core connectivity. Connections should meet all but not limited to voice, latency, jitter, video, frame loss rate, synchronization, classes of service, and traffic separation quality metrics including testing of security (IPsec).	Q-RC-19, 21	White - Comments Solicited			
PSEN Interconnection Testing	A.3.8.2.4.3.6	Testing connections and routing between NPSBN and the PSEs to validate APN connections to PSEN and mobile VPNs.	Q-RC-19, 21	White - Comments Solicited			
Cloud Services Interconnection Testing	A.3.8.2.4.3.7	Testing connections between NPSBN and cloud services. Interconnection testing will include multiple video, telepresence and desktop endpoint type testing across and between FirstNet and selected cloud services networks to test seamless, consistent and deliver excellence from the user's perspective enabling multi-provider, multi-provider(s) interconnection and interoperability for the benefit of FirstNet public safety users.	Q-APP-12	White - Comments Solicited			
Application Certification	A.3.8.2.4.4	FirstNet will have a well-defined test and certification process in place that ensures applications are production grade, free of malware and unintended side effects, and meet the defined performance metrics. The certification process will inform public safety users that the application has undergone to testing and inspection, and can safely be downloaded and used. FirstNet will leverage industry best practices for certification of mobile applications. The contractor(s) will validate the FirstNet Certification process.		White - Comments Solicited			
3rd Party Sandbox Certification	A.3.8.2.4.4.1	The FirstNet Application Developer(s) will test their initial application load in this Pre-certification or Sandbox environment for very limited users. Contractor(s) manages the Sandbox infrastructure, support for Application developer(s) and providing the access to network services, back-end infrastructure etc.		White - Comments Solicited			
FirstNet Hosted Application Certification	A.3.8.2.4.4.2	Once the application is tested on Sandbox environment and validated the contractor(s) shall validate the system level testing on Pre-Production environment for friendly users in Live environment.		White - Comments Solicited			

Configuration Testing	A.3.8.2.4.5	Test the configuration of each equipment in the lab to ensure the network functions normally. Configuration testing is the process of testing the system with each one of the supported software and hardware configurations. The Execution area supports configuration testing by allowing reuse of the created tests.	Q-OPS-4	White - Comments Solicited			
Device Manager Platform Testing	A.3.8.2.4.5.1	Test the device management system for various device functions. The testing of a device management platform is done by simulating the action of thousands of public safety users and detecting and correcting bugs in the applications.	Q-DEV-1, 8	White - Comments Solicited			
RAN Equipment Testing	A.3.8.2.4.5.2	Test the functions of eNB in the lab. During the development of an LTE eNodeB or eNB, a series of different tests are necessary to prove correct operation. After verifying the transmitter and receiver branch, the performance is evaluated to make sure it complies with the requirements covered in the 3GPP technical specifications.		White - Comments Solicited			
Core Network Equipment Testing	A.3.8.2.4.5.3	Test the functions of each EPC equipment in the lab. During the development of an LTE EPC, a series of different tests are necessary to prove correct operation. All the nodes need to comply with the requirements covered in the 3GPP technical specifications.		White - Comments Solicited			
Application Delivery Platform Testing	A.3.8.2.4.5.4	The core infrastructure where the applications are hosted in the Lab shall be tested for various network, application configurations and validated with Mobile Devices, back-end access etc.		White - Comments Solicited			
Service Experience Management	A.3.8.2.4.6	Provide scheduled reports measuring and characterizing the complete user experience with respect to services. Service-level user experience includes monitoring and reporting of specific application performance on devices, application performance across the network, and application performance at all serving nodes. Applications may include video services, 2-way voice calls, downloaded applications from App Stores, etc.	Q-OPS-29	White - Comments Solicited			
Service Experience Data Analytics	A.3.8.2.4.6.1	This function provides usage, location, and performance data analytics in support of Service Experience Management. Experience issues may arise sporadically, or with obscure root cause issues. The ability to perform Data Analytics including analyses of user, service, and application usage and performance behavior across time-of-day, by user type, and other similar metrics are necessary to manage primary and secondary Service Experience Management.	Q-DEV-8, Q-RC-13	White - Comments Solicited			
Service Availability Management	A.3.8.2.4.6.2	Availability management ensures that systems are sized and architected to meet the Service Level Agreements. This includes ensuring proper contingency plans are in place and tested as well as continually reviewing architecture needs in terms of redundancy and high availability based on business needs.		White - Comments Solicited			
Service Capacity Management	A.3.8.2.4.6.3	Capacity management ensures that services are architected with the capacity to meet current and immediate future business capacity needs.		White - Comments Solicited			
Service Level Management	A.3.8.2.4.6.4	Service level management is the identification and monitoring of relevant KPIs to ensure end user quality of service metrics are met or exceeded.		White - Comments Solicited			

Security Systems Management	A.3.8.2.5	The FirstNet National public safety Broadband Network and its agency (PSE) shall be protected for security threats. The security framework shall monitor the threats originating from internal and external domains. Public safety processes sensitive information on a daily basis, which requires robust security measures to ensure integrity, confidentiality, privacy protection, and information assurance. A NPSBN would be an obvious target for cyber attack. This fact requires that extensive security measures be enacted to prevent attacks on the Public safety applications, network to include but not be limited to cyber attacks, physical site security, and denial of service. The FirstNet security policy and Governance shall enforce and meet the PSE applications, devices, configurations and network infrastructure to meet end to end validation, certification which includes both static and dynamic monitoring. The FirstNet National public safety Broadband Network and its agency (PSE) shall be protected for security threats.		White - Comments Solicited			
Physical Security Management	A.3.8.2.5.1	Manage the physical access to all NPSBN locations according to FirstNet's security policies.		White - Comments Solicited			
Personnel Identity Management	A.3.8.2.5.2	Manage the personnel access to all NPSBN locations according to FirstNet's security policies.		White - Comments Solicited			
Cyber Security Monitoring	A.3.8.2.5.3	Monitor the cyber security activities of the NPSBN according to FirstNet's security policies. Security policies developed in collaboration with PSE and other national federal agencies, provides governance and guidance to an organization on managing cybersecurity risk. A key objective of the framework is to encourage state, local PSE to consider cybersecurity risk as a priority, and operational risk while factoring in larger systemic risks inherent to critical infrastructure.	Q-APP-19	White - Comments Solicited			
Security Threat Mitigation	A.3.8.2.5.3.1	Develop procedures, processes, and implement functions in security systems to mitigate against potential security breaches.		White - Comments Solicited			
Public Safety User Security Monitoring	A.3.8.2.5.3.2	Monitoring procedures, processes, and timely implementation of functions in security systems to prevent potential security breaches for public safety users.		Green - FirstNet Only			
Federal User Security Monitoring	A.3.8.2.5.3.3	Monitoring procedures, processes, and timely implementation of functions in security systems in-line with applicable federal security standards to prevent potential security breaches for federal users.		Green - FirstNet Only			
Security Policy Enforcement	A.3.8.2.5.4	Provides Governance on security policy and also policy and procedures related to security threats, mitigation, logging and enforcement capability. FirstNet, Agency and the contractor(s) shall provide the procedure, process for Security Policy enforcement.		White - Comments Solicited			
Public Safety Agency Policy Enforcement	A.3.8.2.5.4.1	Ensuring public safety agencies to comply with FirstNet's security polices and procedures to prevent potential security breaches.		Green - FirstNet Only			
Federal Security Policy Enforcement	A.3.8.2.5.4.2	Ensuring federal agencies to comply with FirstNet's security polices and procedures to prevent potential security breaches.		Green - FirstNet Only			
Disaster Response & Recovery (NIMS Types 1,2,3) & Major Planned Event Operations	A.3.8.2.6	Disaster response and recovery and major event support requires physical assets, human resources, advance planning, and execution protocols to enable rapid response to disaster and major event scenarios. Deployable communication assets are typically used to respond to incidents. Disaster response types are described by FEMA/NIMS, whereas major events are typically pre-planned capacity augmentation scenarios.		White - Comments Solicited			
Network Restoration	A.3.8.2.6.1	Required network restoration results from service impairments involving any aspects of the network. While the majority of restoration efforts typically center around power and backhaul restoration, other physical elements may require restoration while non-physical impairments (including cyber security issues, software, translations) may also require network restoration support		White - Comments Solicited			

Disaster response information gathering	A.3.8.2.6.2	The contractor(s) will support intelligence gathering to understand the specifics of each DR or major event. Information gathered will include event location, scope (geographic and capacity), environmental and access issues, deployment considerations (for example backhaul, power), and estimated event duration.		White - Comments Solicited			
Agency Coordination	A.3.8.2.6.3	Once a disaster event occurs or a major event is planned, the contractor(s) will coordinate deployment of assets and support staff with the lead agency(ies) that require support. The lead agency(ies) may be at the local, state, or federal level.		White - Comments Solicited			
Event Tracking	A.3.8.2.6.4	Disaster Response or major event support will be tracked by the contractor(s) allowing coordination of staff and assets, documentation of support costs, and after action reporting.		White - Comments Solicited			
Event Preparation	A.3.8.2.6.5	The contractor(s) will stage (prepare) staff and assets required to support the disaster recovery or major event based on the completed intelligence gathering and coordination activities.		White - Comments Solicited			
Incident Setup & Management	A.3.8.2.6.5.1	The contractor(s) will deploy the required equipment assets and resources to support the relevant event. The contractor(s) will verify end-to-end functionality of the network assets and work with the local and/or state/federal agencies to manage and maintain network assets during the event.		White - Comments Solicited			
Mitigation Plan Development	A.3.8.2.6.6	Develop plans to deploy mobile assets in a timely manor to restore public safety communications in affected areas. Such items include fuel limitations, damaged access, equipment failure, and backhaul/transport impairments. Plans will be continuously updated based on after action reporting.		White - Comments Solicited			
Mitigation Implementation	A.3.8.2.6.6.1	Mitigation plans will be implemented as required on-site during events and as part of simulated (training) events.		White - Comments Solicited			
Agency Support for Mitigation Plan Development	A.3.8.2.6.6.2	Mitigation plans will need to include required support for local, state, or federal agencies. Training exercises must therefore include representation from these constituents.		Green - FirstNet Only			
Post Incident & Event Analysis Reporting	A.3.8.2.6.7	Post incident/event analysis reporting of major events and disaster scenarios for incorporation into process modifications and training programs to drive and realize continuous improvement for future disaster recovery and major events.	Q-OPS-21	White - Comments Solicited			
Network Monitoring	A.3.8.3	Network monitoring includes the tools and services to monitor network performance (as perceived by the end user) and the status of the network elements providing service to public safety users.		White - Comments Solicited			
National Network Operations Center Management	A.3.8.3.1	The Nation Network Operations Center provides and manages nationwide network monitoring visibility to proactively and reactively resolve issues that may impact user services. The National Network Operations Center serves as the coordination point (managing tier 2-3 teams) to optimize service restoration.		White - Comments Solicited			
Trouble Ticket Management/Coordination	A.3.8.3.1.1	Trouble ticket management includes the ability to enter, log, and track network issues impacting user experience. This function also allows historical reporting to identify performance trends and enable continuous service improvement.	Q-OPS-25	White - Comments Solicited			
Management of Network Events	A.3.8.3.1.2	Network events include any events that can degrade user services or network functionality. Network events can be caused by issues including equipment failure, transport or backhaul service disruption, capacity exhaustion, software issues, or translations issues/errors.		White - Comments Solicited			
Agency Security Operations Center Management	A.3.8.3.2	The contractor(s) will establish protocols working with FirstNet and Agency SOC's to ensure agency applications and data remain secure.		Green - FirstNet Only			
Intrusion Prevention	A.3.8.3.2.1	Prevent security intrusions by proactive and real-time sampling of network traffic and reviewing logs to detect and eliminate in-progress and future threats.		White - Comments Solicited			
Intrusion Recovery	A.3.8.3.2.2	Recovery from security intrusions by proactively removing malware or other security threats from the NPSBN and documenting how the intrusion occurred and steps required to prevent reoccurrence.		White - Comments Solicited			
Internal Security Compromise Detection	A.3.8.3.2.3	Detecting threats originating from within the trusted network or system.		White - Comments Solicited			
External Security Intrusion Detection	A.3.8.3.2.4	Detecting threats originating from outside the trusted network.		White - Comments Solicited			

Federal Security Operations Center Management	A.3.8.3.3	Communications management between the federal security operations center and the NPSBN security center.	Q-OPS-12	White - Comments Solicited			
NPSBN Security Operations Center Management	A.3.8.3.4	Monitoring, detecting, and resolving incidents that may affect the confidentiality, integrity, or availability of network devices, end-user devices, and systems.	Q-OPS-12	Green - FirstNet Only			
NPSBN Security Intrusion Monitoring & Detection by SOC	A.3.8.3.4.1	Surveillance and identification that an unauthorized access attempt has been made, is occurring, or has occurred.		Green - FirstNet Only			
Device Malware Detection and Deletion	A.3.8.3.4.2	Software and monitoring functionality to identify and correct (or isolate) malware located on user devices.		White - Comments Solicited			
Field Testing for Public Safety Services	A.3.9	Field testing and verification of public safety user and PSE experience in various geographies across the US and under conditions that are relevant to public safety. This is a key verification on public safety service quality assurance for FirstNet and feedback to contractors.		White - Comments Solicited			
Public Safety Use Case Testing and Verification	A.3.9.1	Field testing and verification of public safety use cases (including experience quality such as voice quality) in various geographies across the US and under relevant conditions. Primary purpose is to ensure an acceptable service level of public safety experience for all use cases		White - Comments Solicited			
Public Safety User Experience Assurance & Verification	A.3.9.2	Field testing and verification of public safety network services (technical support, user provisioning, service response times, service usability) in various geographies across the US and under relevant conditions. Primary purpose is to ensure an acceptable service level of public safety experience for all use cases		White - Comments Solicited			
Public Safety Service Quality and Capability Assurance	A.3.9.3	Field testing and verification of public safety network services (dynamic QPP, local control, device usability) in various geographies across the US and under relevant conditions. Primary purpose is to ensure an acceptable service level of public safety experience for all use cases		White - Comments Solicited			
Policies and Procedures	A.4	Define policies and procedures focused on business processes related to provisioning, billing, certification, profiles, deployment and operational guidelines.	Q-DEV-1, Q-RC-2	White - Comments Solicited			
Define, Monitor, & Implement Provisioning Policies & Procedures	A.4.1	Provide the provisioning policies and procedures relating to subscription management of agencies and users.		White - Comments Solicited			
Define, Implement, & Monitor Network Policies & Procedures	A.4.2	Develop, implement, and monitor overall operating policies and procedures for the NPSBN fully compliant with all laws, rules, standards, and regulations, applicable to FirstNet.		White - Comments Solicited			
Define & Implement Operational Procedures	A.4.2.1	Define operational procedures to be implemented throughout NPSBN. These operational procedures would provide guidance to field teams on the optimal methods to ensure network performance meets all NPSBN requirements.		White - Comments Solicited			
Monitor Operational Procedure Compliance	A.4.2.2	Monitor and provide feedback to support the improvement of network operating procedures.		Green - FirstNet Only			
Define Standard Policies for User Profiles	A.4.3	Develop the user policy profile framework which includes static, dynamic, and subscription profiles.	Q-DEV-1, Q-RC-2	Green - FirstNet Only			
Static QPP Profile Definition	A.4.3.1	Develop the user policy profile framework specifically for static, non-emergency situations.	Q-RC-2	Green - FirstNet Only			
User Subscription Profile Definition	A.4.3.2	Define all user subscription profiles for NPSBN services such as voice, data, push-to-talk.	Q-DEV-1, Q-RC-2	Green - FirstNet Only			
Dynamic QPP Profile Definition	A.4.3.3	Develop the user policy profile framework specifically for dynamic, emergency situations.	Q-RC-2	Green - FirstNet Only			
Define, Monitor, & Implement Billing Policies & Procedures	A.4.4	Provide the policy and procedures related to billing subscription and their rate plans for both home and roaming scenarios.		White - Comments Solicited			
Develop Best Practices	A.4.5	Define best practices for security, industry standards on processes, network and business operations incorporating agency and state key learnings.		White - Comments Solicited			
Develop Customer Care Policies & Procedures	A.4.6	Development of policies and procedures related to the support and care of users including account management, resolving user issues, and billing.		White - Comments Solicited			
Develop Marketing Policies & Procedures	A.4.7	Developing and managing marketing policies and procedures in consultation with states and agencies.		White - Comments Solicited			

Develop Sales Policies & Procedures	A.4.8	Developing and managing sales policies and procedures in consultation with the provider(s) and states.		White - Comments Solicited			
System Engineering Oversight	A.4.9	Oversee systems engineering within NPSBN to ensure compliance of the engineering lifecycle and evolution of the NPSBN.		Green - FirstNet Only			
Implement & Enforce Policy Procedures Across Agencies	A.4.10	Implement and enforce FirstNet security policies, business processes, and operational procedures within the local agencies.		Blue - Public Safety			
NPSBN Services Program Management & Contract Compliance	A.5	The provider(s) will provide a program management function that interfaces with the FirstNet PMO. It will follow general program management practices, and manage performance, delivery, and reporting on the overall program.		White - Comments Solicited			
Agency Administration Program Support	A.5.1	Responsible for coordinating with state, federal, tribal, or other agencies for any agency-specific program needs or reporting.		White - Comments Solicited			
Services Program Support & Reporting	A.5.2	Responsible for managing a portfolio of services. This includes service roadmap planning, usage reporting, and new service definition.		White - Comments Solicited			
Network Operation Program Support	A.5.3	Providing network operation strategy, planning, and reporting. This includes status on life cycle events. The provider(s) will coordinate network operations across FirstNet, public safety entities and any roaming provider(s) or related carriers. The provider(s) will also be responsible for maintaining operations consistent with the QASP.		White - Comments Solicited			
Contract Financial Administration	A.5.4	Responsible for managing and reporting the financial performance of the network solution contracts, including financial variance reporting, forecasting, and change management.		White - Comments Solicited			
Revenue Variance Reporting	A.5.4.1	Responsible for generating reports detailing the differences between actual revenue and planned revenue for public safety use, inclusive of all NPSBN revenue generating products, services, device sales/leases, etc.		White - Comments Solicited			
Cost Variance Reporting	A.5.4.2	Responsible for the reporting of the difference between budgeted cost of work performed, and the actual cost of work performed.		White - Comments Solicited			
Cost of Sales Reporting	A.5.4.2.1	Responsible for the reporting of the accumulated total of all costs used to create a product or service, which have been sold. The various costs of sales fall into the general sub-categories of direct labor, materials, and overhead and may also be considered to include the cost of commissions associated with a sale.		White - Comments Solicited			
General & Administrative Cost Reporting	A.5.4.2.2	Reporting of expenditures related to sales, general and administrative costs.		White - Comments Solicited			
Contract Performance Tracking	A.5.4.3	Responsible for tracking the financial performance of the contract for the implementation of the network solutions.		White - Comments Solicited			
Regulatory Management	A.5.5	Ensure all activities performed by the contractor(s) in relation to the rollout of the NPSBN follows all the applicable regulatory procedures. Provide regular reporting to FirstNet on all regulatory matters including any changes to past filings		White - Comments Solicited			
Preparation of Regulatory Filings and Forms	A.5.5.1	Ensure contractor(s) completes all regulatory forms for filing in relation to the rollout of the NPSBN in time, and delivers these to FirstNet for review and approval. This includes new filings and changes to past filings. Contractor(s) will file the regulatory forms to the appropriate authorities after receiving approval from FirstNet		White - Comments Solicited			
NBPSN Regulatory Compliance Monitoring & Reporting	A.5.5.2	Ensure all activities performed by the contractor(s) in relation to the rollout of the NPSBN complies to all applicable regulatory obligations of FirstNet. Provide regular reporting to FirstNet on all regulatory matters including any changes to past filings		White - Comments Solicited			
Reporting of Opt-Out State Compliance	A.5.5.3	Monitor the performance of opt-out states in relation to laws, regulations, and technical compliance pertaining to the rollout of the NPSBN. Provide regular reporting to FirstNet on the performance of opt-out states		White - Comments Solicited			
Legal Support	A.5.6	Provide any legal support necessary to FirstNet in relation to the rollout and performance of the NPSBN and contract. Provide supporting documentation on any legal hearings that may be necessary for FirstNet to attend		White - Comments Solicited			
Legal Compliance Monitoring & Reporting	A.5.6.1	Ensure all activities performed by the contractor(s) in relation to the rollout of the NPSBN complies to all legal obligations under the law applicable to FirstNet. Provide regular reporting to FirstNet on all legal matters that pertain to FirstNet		White - Comments Solicited			

Sales Management	A.6	Responsible for working with the provider(s) on the sales strategy and framework for public safety devices and services		White - Comments Solicited			
Public Safety Entity Sales Channel Management	A.6.1	Responsible for agreeing with provider(s) on overall sales targets and performance for devices and services		White - Comments Solicited			
Local Sales	A.6.1.1	Responsible for working with public safety agencies on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
Law Enforcement Sales	A.6.1.1.1	Responsible for working with law enforcement agencies on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
Fire Department Sales	A.6.1.1.2	Responsible for working with Fire departments on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
EMS Sales	A.6.1.1.3	Responsible for working with Emergency Medical Service agencies on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
911 Sales	A.6.1.1.4	Responsible for working with 911 service centers on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
Others Entity Sales	A.6.1.1.5	Responsible for working with other public safety related agencies or entities on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
Federal Sales	A.6.1.2	Responsible for working with Federal Government departments on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
Federal Public Safety Sales	A.6.1.2.1	Responsible for working with Federal Government public safety departments on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
Federal Non Public Safety Sales	A.6.1.2.2	Responsible for working with Federal Government non-public safety departments on sales, service performance and soliciting inputs on evolving requirements for devices and services		White - Comments Solicited			
State Government and Tribal Sales	A.6.1.3	Responsible for working with State Government and Tribal organizations on sales, service performance and soliciting inputs on evolving requirements for devices and services.		White - Comments Solicited			
State Government and Tribal Public Safety Sales	A.6.1.3.1	Responsible for sales activities and user acquisition within state government and tribal organizations.		White - Comments Solicited			
State Government and Tribal Non Public Safety Sales	A.6.1.3.2	Responsible for sales activities and user acquisition within non public safety of state government and tribal organizations.		White - Comments Solicited			
Retail Sales	A.6.1.4	Responsible for sales activities and user acquisition within the retail channel.		White - Comments Solicited			
Retail/Provider(s) Sales	A.6.1.4.1	Responsible for sales activities and user acquisition within the retail provider(s) channel.		White - Comments Solicited			
Retail/3rd Party Sales	A.6.1.4.2	Responsible for sales activities and user acquisition within the 3rd party retail channel.		White - Comments Solicited			
Internet and Telemarketing Sales	A.6.1.5	Responsible for indirect sales channels and soliciting inputs on evolving requirements for devices and services.		White - Comments Solicited			
Utility Responder Sales	A.6.1.6	Responsible for working with private sector sales channels on sales and evolving requirements for devices and services.		White - Comments Solicited			
Sales to Utilities	A.6.1.6.1	Responsible for working with utility sales channels on sales and evolving requirements for devices and services.		White - Comments Solicited			
Account Management	A.6.1.7	Responsible for the strategy on account management for pre and post sales and marketing.		White - Comments Solicited			
Customer Acquisition Planning & Implementation	A.6.1.7.1	Responsible for the strategy on customer acquisition through promotions, sales channels, and collateral.		White - Comments Solicited			
Customer Retention & Winback Planning and Implementation	A.6.1.7.2	Responsible for the strategy on customer retention and winback.		White - Comments Solicited			
Account Planning	A.6.1.7.3	Development of the strategy for account planning regarding sales and on-going account management.		White - Comments Solicited			
Special Pricing Development	A.6.1.7.4	Development of special pricing offers for enterprise.		White - Comments Solicited			
User Migration and Evolution	A.6.1.8	Supports the migration of users from existing LMR, public safety private wireless networks, opt-out states networks, and commercial networks to the NPSBN.		White - Comments Solicited			

Sales Operations & Support	A.6.2	Responsible for developing the framework together with the provider(s) for an efficient sales operation and support service		White - Comments Solicited			
Sales Reporting	A.6.2.1	Monitor and produce high level management reports on the performance of sales channels	Q-BUS-4	White - Comments Solicited			
Compensation Planning and Implementation	A.6.2.2	Develop with a sales channel compensation strategy and oversee the implementation		White - Comments Solicited			
Sales Training	A.6.2.3	Develop with provider(s) a sales training program and oversee its successful implementation		White - Comments Solicited			
Service Fulfilment	A.6.2.4	Develop with provider(s) a process to ensure fulfilment of services and devices and oversee its successful implementation		White - Comments Solicited			
Sales Planning	A.6.3	Together with the provider(s), develop sales plans for all segments of customers		White - Comments Solicited			
Define the Sales Strategy and Ensure Compliance	A.6.3.1	Together with the provider(s), develop the strategic framework for the successful implementation of the sales plans for all segments of customers and monitor its performance	Q-BUS-4	White - Comments Solicited			
Sales Forecasting	A.6.3.2	Develop with provider(s) a short and long term sales forecast and adjust according to changing market trends and dynamics		White - Comments Solicited			
Establishing Sales Targets with Partners and Monitoring Performance	A.6.3.2.1	Develop short and long term sales forecast and adjust according to changing market trends and dynamics. Measure target performance achievements	Q-BUS-4	Green - FirstNet Only			
Results Reporting/Trending	A.6.3.2.2	Perform to meet expected short and long term sales forecast and adjust according to changing market trends and dynamics.		White - Comments Solicited			
Sales Monitoring and Compliance	A.6.3.3	Develop with provider(s) and stakeholders a standard sales performance monitoring framework and ensure timely distribution of sales reports	Q-BUS-4	Green - FirstNet Only			
Major Accounts Management	A.6.4	Develop major accounts strategy and monitor and produce high level management reports on major accounts performance		White - Comments Solicited			
Sales Engineering Support	A.6.5	Provide customized engineering support for major accounts and projects		White - Comments Solicited			
Facilitate Product Demonstrations	A.6.5.1	Provide capability to demonstrate products/services to end-users		White - Comments Solicited			
Support Sales Efforts	A.6.5.2	Provide customized engineering support for sales efforts on major accounts		White - Comments Solicited			
Support RFP Development Efforts	A.6.5.3	Provide customized engineering support for sales proposals and projects		White - Comments Solicited			
Provide Product Feedback to Engineering	A.6.5.4	Responsible for providing information on technical and operational issues		White - Comments Solicited			
Product Management	A.7	Product management defines, plans, obtains the acceptance for the portfolio of services, applications, and features to meet First Responder requirements.		White - Comments Solicited			
Network Services Portfolio Management	A.7.1	Create and maintain a network services portfolio management process for existing and future features of network services and their components. The feature roadmap will be developed and maintained with input from all key stakeholders including operations, outreach, and governance teams, public safety users, developers, et al.		White - Comments Solicited			
Application Developer Ecosystem Product Life Cycle Management	A.7.1.1	Manage the necessary software tools, test environments, and processes to support developers allowing them to easily develop, publish, and be compensated for their applications. This includes enhancing the products and services over time in the Application Developer Ecosystem		White - Comments Solicited			
Application Publishing Management	A.7.1.1.1	Manage the application publishing process so developers can easily publish application to the FirstNet Application Store. This includes supporting application upgrades, application discovery and different forms of payment for applications.	Q-APP-4	White - Comments Solicited			
Application Upgrading Management	A.7.1.1.1.1	Manage and provide the software tools and processes to provide version control for applications being developed for the FirstNet Application Store. Support updates to applications and managing the way application updates are made available to users. This function also includes notifying developers when changes and enhancements are being made to APIs or SDKs that might impact them.	Q-APP-4	White - Comments Solicited			

Application Discovery Management	A.7.1.1.1.2	Manage and provide a directory of new and existing applications and services available to agency or individual subscribers. Permissions may be set on what an agency or individual is authorized to view and select to download based on the agency, individual, and device.	Q-APP-4	White - Comments Solicited			
Application Purchasing Management	A.7.1.1.1.3	Manage and provide the necessary APIs on a service delivery platform to allow the FirstNet Application Store or individual applications to charge for application purchases. This includes supporting as one-time purchases, Monthly Recurring Charge (MRC), Annual Reoccurring Charge (ARC), one time payments, in app charges, etc. Charges will be reflected on a subscribers of agencies bill.		White - Comments Solicited			
Application Review/Rating Systems Management	A.7.1.1.2	Manage and provide the ability for agencies and individuals to review capabilities and functionality of an application before purchasing and downloading. Provide a rating system of applications, that users can provide there comments and reviews to.	Q-APP-4	White - Comments Solicited			
Provide Developer Support	A.7.1.1.3	Provide software SDK and API libraries, coding examples, test environments, webinars and events, and development process to launch. Only registered developers will have access to these facilities. This should include forums and the ability to get developer support from experienced application developers (i.e. developer customer service).	Q-APP-7	White - Comments Solicited			
Application Fraud Management	A.7.1.1.4	Provide mechanisms for the detection, prevention, and notification of application fraud. Processes to rapidly discontinue use and withdrawal of fraudulent application from devices and application stores.		White - Comments Solicited			
Location Services Product Life Cycle Management	A.7.1.2	Management of a location services infrastructure which provides FirstNet with both user (SUPL/LPP) and control (LPP) plane location capabilities for asset management and emergency public safety user location services. This function should include "z" direction and relevant (indoor and outdoor) accuracy levels.		White - Comments Solicited			
IT Services Product Life Cycle Management	A.7.1.3	Enable general IT service, e.g. not specific to wireless, used by many IT infrastructure components within FirstNet's network domain(s).		White - Comments Solicited			
Domain Name Service (DNS) Management	A.7.1.3.1	Enable a Domain Name Service (DNS) that translates domain names to the numerical IP addresses in accordance with all relevant RFCs.		White - Comments Solicited			
Enterprise Security Management	A.7.1.3.2	Enable the security components, policies, and procedures to protect the IT network from cyber attack, loss and exposure of sensitive information, and from other threats to the security of the FirstNet domain that may impact the network itself, the users, or the age. The IT network security framework and solutions should be compatible and coordinate with security solutions applicable to the rest of the FirstNet solution.	Q-APP-19	White - Comments Solicited			
Digital Certificate Management	A.7.1.3.2.1	Issuance and revocation of trusted certificates based on PKI for validation of server and device endpoints, users, and encrypting information. FirstNet may be its own certificate authority or connected to the Federal Bridge. This service should include multiple classes of certificates and multiple types of certificates.		White - Comments Solicited			
Identity Management Product Life Cycle Management	A.7.1.4	User Identity Management provides authentication and authorization services that ensure users have been properly vetted and approved before they are granted access to services, applications and/or resources. Identity Management includes the creation and management of policies which define the access constraints, ensure that user actions are properly audited and logged. Identity management is as much about enabling access to authorized users as it is about denying access to unauthorized users.		White - Comments Solicited			
Identity Management Auditing & Accounting	A.7.1.4.1	Auditing and Accounting of Identity Management provides audit log reporting and management to enable reconstruction and examination of the sequence of activities surrounding, or leading to, a specific operation, procedure, or event from inception to final result. Auditing and Accounting also generates searchable audit data and provides for reporting mechanisms that include alerts.		White - Comments Solicited			

Federated Identity Management	A.7.1.4.2	Federated Identity Management provides the ability for users, systems and services in one domain or agency to get access to services and applications in a different domain or agency. Federated Identity Management requires standardization of the authentication and authorization methods and interfaces which allows for users, services and applications to interoperate across security boundaries (e.g. domains, agencies, etc.). Federated Identity Management allows for collaboration and reuse across agencies.		White - Comments Solicited			
Identify Trustmarks Management	A.7.1.4.2.1	The Identify Trustmarks function is for the identification of Trustmarks that should be supported as part of the FirstNet Federated Identity Management solution. Trustmarks include specific Identity related functionality, and the purpose of this function is to identify specific Trustmarks that are recommended to be supported across agencies in order to more easily achieve secure access and interoperability (i.e. federated identity management).		Green - FirstNet Only			
Defining & Evolve Trustmarks	A.7.1.4.2.2	The Define & Evolve Trustmarks function is for the creation, updating and vetting of Trustmarks that are then recommended to be included in the FirstNet Federated Identity Management solution. The Trustmarks should be derived and adopted from standards where possible. Evolving the Trustmarks ensure that the FirstNet identity management solution is always improving with a goal to promote best of breed Trustmarks.		White - Comments Solicited			
Define and Support Access Policies	A.7.1.4.3	Access Policies are used by the Authorization Services and provide the access constraints, rules and details for applications, services and resources. Access Policies are dynamic and can be created, updated and removed. Access policies can be shared across multiple resources, and should be standardized and normalized for FirstNet where possible. An example of a standardized access policy would be one written in extensible Access Control Markup Language (XACML). A standardized format for access policies should be used so they can easily be validated and shared by different resources. The applications and services provided by local agencies must make use of these policies. Agencies must be able to tailor these policies for applications and services for which they have local control.		White - Comments Solicited			
PSE Support and Define Local Access Policies	A.7.1.4.3.1	PSEN provides the support and definition of their local access policies for the set up and establishment of PSEN Identity management		Blue - Public Safety			
Support and Define Global Access Policies	A.7.1.4.3.2	FirstNet provides the support and definition of global access policies for the set up and establishment of global Identity management		Green - FirstNet Only			
Manage Authorization Services	A.7.1.4.4	Authorization Services ensure that users are authorized (i.e. explicitly approved), before being given access to an application, service, or resource. The authorization services make use of Access Policies in order to make the access decision. Unique access policies can be assigned to applications, services and resources. Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs) are an example of software that provide authorization services. The Authorization Services should be provided in a flexible, extensible, and standardized manner where possible.		White - Comments Solicited			
Manage Authentication Services	A.7.1.4.5	Authentication Services ensure that users are properly identified before authorized. Multiple authentication mechanisms may exist and each one may have a different strength or level of assurance associated with it. Authentication services ensure that unknown users are differentiated from known users to enable proper authorization to occur. The Authentication Services should be provided in a flexible, extensible, and standardized manner where possible, and allow public safety agencies and applications developers to leverage the authentication services in an Identity as a Service (IdaaS) manner.		White - Comments Solicited			

Manage Multi-Factor Authentication	A.7.1.4.5.1	Multi-Factor Authentication functions include username/password, PKI Certificate, Biometrics, etc., within the authentication framework. Applications/services may choose to require different authentication methods be used together (i.e. multi factor) in order for a client to be properly authenticated. An example of this would be to require both a pin and a biometric as part of the authentication process. The authentication services that are provided must support multifactor authentication, and should be customizable by the application/service developer that is leveraging the authentication services.		White - Comments Solicited			
Manage Single Sign-on	A.7.1.4.5.2	Single Sign-on (SSO) provides the ability for a user to authenticate once, and then be provided with access to services, applications, and resources in any domain offering resources to which that user is authorized without having to re-authenticate. This functionality must leverage community standards and specifications and provide SSO access into devices as well as applications and services that are accessed through browsers or native applications on any device.		White - Comments Solicited			
Group Communication (GCSE 3GPP) Product Life Cycle Management	A.7.1.5	Manage the group communications life cycle from launch including it's evolution roadmap to develop an efficient mechanism to distribute the same content to multiple users. GCSE enables group communication services for voice, video, and data communication for groups of users.		White - Comments Solicited			
QoS, Priority, and Preemption (QPP) Administration	A.7.1.6	Defines, plans, obtains the acceptance for the QoS, Priority, and Pre-emption mechanisms. Centralized authorization, identity management, and subscriber information and QoS, Priority, and Pre-emption policies would be employed to manage the distribution of control across the agency/FirstNet touch points.	Q-RC-2	White - Comments Solicited			
Management and Enablement of Dynamic User Profiles	A.7.1.6.1	Dynamic Incident Management allows QPP administration capable of performing real time changes to application and user profiles, leading to QCI, ARP and Access Class barring changes, in the course of an incident and returning the public safety users to their pre-incident levels following the completion of the incident.	Q-RC-2	White - Comments Solicited			
Management of Access Class Barring	A.7.1.6.1.1	Access Class Barring includes the implementation of a nationwide scheme for assigning Access Classes to public safety users and secondary users following the 3GPP recommendations in TS 22.011, Section 4.2 within QPP administration.	Q-RC-2	White - Comments Solicited			
Management of QoS Class Identifiers (QCI)	A.7.1.6.1.2	Enable and support of all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.	Q-RC-2	White - Comments Solicited			
Immediate Peril Service Management	A.7.1.6.1.3	This network services allows for the immediate raising of priority for first responders who activates his or her immediate peril button. Public safety will define the order of services and their priority following the invocation of immediate peril and QPP administration application function must be capable of executing this in real-time and returning the public safety user to its pre-immediate peril profile following the clearing of this state. The service will provide immediate location of the first responder(s) who active their immediate peril button(s)	Q-RC-2	White - Comments Solicited			
Allocation and Retention Policy (ARP) Management	A.7.1.6.1.4	This network service defines support for the usage of all 15 ARP values defined in 3GPP and ARP pre-emption capability and vulnerability functions as defined in 3GPP 23.203 within QoS, Priority, Pre-emption administration.	Q-RC-2	White - Comments Solicited			
Incident Command System (ICS) Service Management	A.7.1.6.1.5	Product development support for ICS services as required by FirstNet. The Incident Command System (ICS) is a management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.	Q-RC-2, 13	White - Comments Solicited			
Real Time Priority & Role based QoS Execution	A.7.1.6.1.5.1	This network service provides administration of real time priority and role based QoS changes (leading to QCI, ARP and/or Access Class barring changes) in the course of an incident and returning the public safety users to their pre-incident levels following the completion of the incident.	Q-RC-2	White - Comments Solicited			

Processing of Responder Emergency Invocation	A.7.1.6.1.6	This network services supports the immediate raising of priority for a first responder who activates his or her responder emergency button. Public safety will define the order of services and their priority following the invocation of responder emergency and QPP administration application function must be capable of executing this in real-time and returning the public safety user to its pre-responder emergency profile following the clearing of this state.	Q-RC-2	White - Comments Solicited			
Implementation of Immediate Location & Priority	A.7.1.6.1.6.1	This service allows for the immediate raising of priority for first responders who activates his or her responder emergency button and the immediate emergency location request of the public safety user by the network. Public safety will define the order of services and their priority following the invocation of responder emergency and immediate location. The QPP application and location function must be capable of executing these requirements in real-time and returning the public safety user to its pre-responder emergency profile following the clearing of this state.	Q-RC-2	White - Comments Solicited			
Management and Enablement of Static User Profiles	A.7.1.6.2	Create and manage QPP profiles that include a user's static QPP configuration (including QCI, ARP, QBR, GBR, APN-AMBER, and UE-AMBER) to meet FirstNet's first responder needs. These needs include users being able to communicate and access PS applications during incidents.	Q-RC-2	White - Comments Solicited			
Payment Services Product Life Cycle Management	A.7.1.7	Manage the product life cycle of the payment feature and capability incorporated in all relevant services and applications provided by the NPSBN		White - Comments Solicited			
Presence Services Product Life Cycle Management	A.7.1.8	Presence Services includes the creation of a presence infrastructure. The solution should be compliant with GSMA Rich Communications recommendations (RCS) and aggregate and deliver real-time presence information including user availability, service capability, and social presence for associated public safety contacts and groups across FirstNet.	Q-RC-2, 13	White - Comments Solicited			
Local Status Update Provisioning	A.7.1.8.1	Provide a local, constantly updated, personalized "home page" for subscribers providing information such as real-time presence information about local FirstNet users, groups, subscribed applications, events, and incidents.		White - Comments Solicited			
Mobile Device Management Product Life Cycle Management	A.7.1.9	Plan the different levels of device management control at the national, regional and local PSEN levels. Provide the necessary extensions for public safety in conjunction with device testing. Continue to add new capabilities as public safety needs evolve.		White - Comments Solicited			
User Services Portfolio Management	A.7.2	Manage and configure the portfolio of user services, on a per-user or per-group basis, which applications are authorized for use by the PSE's users.	Q-RC-9, 29	White - Comments Solicited			
Mission Critical Push-to-talk Voice (3GPP) Product Life Cycle Management	A.7.2.1	Manage the product life cycle for the mission critical push-to-talk services including following and supporting the development of the service in Standards to ensure synchronization with Firstnet and public safety requirements		White - Comments Solicited			
Security Management for Push to Talk Services	A.7.2.1.1	Manage the product life cycle for the mission critical push-to-talk security services including following and supporting the development of the service in Standards to ensure synchronization with Firstnet security standards and guidelines		White - Comments Solicited			
Group Management/Communications Service Management	A.7.2.1.2	Manage the product life cycle for the group communications capabilities in the NPSBN including following and supporting the development of the service in Standards to ensure synchronization with Firstnet and public safety requirements		White - Comments Solicited			
Broadcast Services Product Life Cycle Management	A.7.2.2	This function will use a new technology called eMBMS to optimize bandwidth required for broadcast, a type of one to many communications.		White - Comments Solicited			
Data Services Product Life Cycle Management	A.7.2.3	Data services are the PS services that are standard-based, uniform means of accessing information in a form useful to PS applications. It also includes video or telemetry. A key requirement for data services is that they abstract the data from its physical persistence structure in the PS database, presenting it in a form that is most useful for PS applications.		White - Comments Solicited			

Video Services Product Management	A.7.2.3.1	Video services are similar to data services except that the information returned from the PS applications are distributed in video clips or other multimedia format. It is expected much of the information needed by emergency responders includes both pictures and sound.		White - Comments Solicited			
Mobile Video Feeds Service Management	A.7.2.3.1.1	The video feed would allow command post and Emergency Operations Center (EOC) personnel to visualize the incident scene in relation to damage and apparent needs when compared to other incident scenes. Mobile video feed is vehicle-mounted video.		White - Comments Solicited			
3rd Party Video Service Management	A.7.2.3.1.2	This is a function the NPSBN will support so as to interface with fixed video sources from third-party systems, such as facility security cameras.		White - Comments Solicited			
Video Feeds Service Management	A.7.2.3.1.3	There are many fixed video feeds that are vital to public safety and first responders completing their jobs efficiently and safely. These feeds must be available for consumption by FirstNet users who have the proper privileges to access them.		Blue - Public Safety			
CMAS Services Product Management	A.7.2.3.2	The Commercial Mobile Alert System (CMAS) is part of the Integrated Public Alert and Warning System (IPAWS) that allows designated government entities to deliver warning notifications (alerts) to commercial wireless users. CMAS is defined by the FCC's First, Second, and Third Report and Order in the "Matter of the Commercial Mobile Alert System" as an optional service allowing the commercial wireless operators to voluntarily comply and provide CMAS services to their subscribers.		White - Comments Solicited			
Alert Aggregation Service Management	A.7.2.3.2.1	The CMAS network allows the Federal Emergency Management Agency (FEMA) to aggregate alerts from different sources and send them over a secure interface to participating wireless service providers who in turn will send these emergency alerts as text messages to their subscribers.		White - Comments Solicited			
Alert Dissemination Service Management	A.7.2.3.2.2	The CMAS network allows the Federal Emergency Management Agency (FEMA) to disseminate alerts from different sources and send them over a secure interface to participating wireless service providers who in turn will send these emergency alerts as text messages to their subscribers.		White - Comments Solicited			
Local Delivery Service Management	A.7.2.3.2.2.1	The interface between the Cell Broadcast Center (CBC) and Mobility Management Entity (MME) provides warning message delivery and control functions. 3GPP TS 23.401 provides the procedures for Stage 2 information flows for warning message delivery and warning message cancel. It also provides the architecture and local warning message delivery to a notification area and control functions support CMAS.		White - Comments Solicited			
Messaging Product Management	A.7.2.3.3	This function includes text messaging, multimedia messaging, and any messaging service needed by PS.		White - Comments Solicited			
Email Service Management	A.7.2.3.3.1	Electronic mail, most commonly referred to as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Email operates across the Internet or other computer networks. The email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages.		White - Comments Solicited			
Instant Messaging Service Management	A.7.2.3.3.2	Instant messaging (IM) is a type of online chat which offers real-time text transmission over the Internet. Some IM applications can use push technology to provide real-time text, which transmits messages character by character, as they are composed. More advanced instant messaging can add file transfer, clickable hyperlinks, Voice over IP, or video chat.		White - Comments Solicited			

SMS/MMS Service Management	A.7.2.3.3.3	Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages. SMS was the most widely used data application, with an estimated 3.5 billion active users, or about 80% of all mobile phone subscribers at the end of 2010. Multimedia Messaging Service (MMS) is a standard way to send messages that include multimedia content to and from mobile phones. It extends the core SMS (Short Message Service) capability		White - Comments Solicited			
M2M Feeds Product Management	A.7.2.3.4	Machine to Machine (M2M) refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. M2M is considered an integral part of the Internet of Things (IoT) and has a wide range of PS applications for emergency responders.		White - Comments Solicited			
Mission Critical Data Service Management	A.7.2.3.4.1	Manage the transmission of data that is critical to the FirstNet mission, in a manner that meets FirstNet's defined SLA's. Failure of transmitting mission critical data will result in the failure of emergency rescue and public safety operations.		White - Comments Solicited			
Non-Mission Critical Data Service Management	A.7.2.3.4.2	This is a function to transmit routine data, the data that is not crucial to the FirstNet mission as described above.		White - Comments Solicited			
Cloud Services/Hosted Applications Management	A.7.2.3.5	This function is for FirstNet to operate and manage the Cloud offering that includes Software as a Service, Infrastructure as a Service, and Platform as a Service that can be used by public safety agencies and applications. SLA's and security requirements will be established in which the FirstNet Cloud must meet.	Q-APP-12	White - Comments Solicited			
Manage Software as a Service (SaaS)	A.7.2.3.5.1	This function is provide, operate and manage the value added Software as a Service offerings made available to public safety agencies. The software must be developed, updated and evolved to meet the agencies needs, and can include agency applications, identity services, data processing services, etc. This includes the Agency Homepage, and other cloud software services that are made available to users.		White - Comments Solicited			
Manage Big Data Analytics Platform	A.7.2.3.5.2	This function is to provide, operate and manage a Big Data and analytics platform for use by agencies and application developers. The platform must be multi-tenanted and meet the FirstNet data security requirements and SLA's. A continually evolving set of analytical services must be made available to the users of the platform. The analytics provide additional value added information to users by analyzing historical and real-time data and/or patterns in the data. This capability is part of the Cloud services that are offered to agencies and users.		White - Comments Solicited			
Manage Agency Information Homepage	A.7.2.3.5.3	This function provides the operation and management of the agency configurable and customizable Information Home Page for each agency to use to serve as a landing page for it's users. The Information Home Page must include the ability to authenticate users and restrict access to information based on user attributes. Additionally it must be able to expose agency incident and situational awareness information, as well as agency and network status and alerts. Agency administrators can add content to their home page, and tailor the out of the box capabilities so the information that is displayed is relevant for their agency		White - Comments Solicited			
Manage Service Delivery and Installation	A.7.2.3.5.4	This function is for the management, delivery configuration and installation of the FirstNet Cloud Services. FirstNet offers a variety of 'X' as a Service tools and software to public safety agencies and application developers, and this function ensures that support is provided to the users of those services.		White - Comments Solicited			
Manage Infrastructure as a Service (IaaS)	A.7.2.3.5.5	This function is provide, operate and manage cloud Infrastructure as a Services that are made available to public safety agencies. The Infrastructure as a Service is used for application hosting for agency and 3rd party applications and services. The application hosting must meet the FirstNet security requirements and SLA's.		White - Comments Solicited			

Cloud Service Discovery Management	A.7.2.3.5.6	This function manages and provides the ability to the public safety agencies, application developer and cloud users to easily discover and use the services that are provided by the FirstNet Cloud. The cloud services may require purchase to use, and information about SLAs for the cloud services must be available to users.		White - Comments Solicited			
Direct Mode Product Life Cycle Management	A.7.2.4	This function is the same as Proximity Services. Direct Mode (DM) is the communication method between two PS devices in the Band 14 spectrum. This kind of communication is similar to walkie talkie. It does not require access to the network.		White - Comments Solicited			
Voice Services Product Life Cycle Management	A.7.2.5	This function provides the public safety users the voice communication services, either in the form of stand circuit based voice or voice over IP. This service will be delivered in the LTE based NPSBN.		White - Comments Solicited			
Cellular Telephony Product Management	A.7.2.5.1	Voice services available over commercial cellular networks. The NPSBN can enable Voice-over-IP (VoIP) telephony and other open-standard telephony solutions.		White - Comments Solicited			
Call Forwarding Service Management	A.7.2.5.1.1	Call forwarding, or call diversion, is a telephony feature of some telephone switching systems which redirects a telephone call to another destination, which may be, for example, a mobile telephone, voicemail box or another telephone number where the desired called party is available.		White - Comments Solicited			
Voice Mail Service Management	A.7.2.5.1.2	The NPSBN shall support telephony voicemail service. On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the use of voicemail service. The voicemail service SHALL support a per-user passcode, which must be entered by the NPSBN-U prior to the management of voicemail message.		White - Comments Solicited			
Ring back tones Service Management	A.7.2.5.1.3	A ringback tone (or ringing tone) is an audible indication that is heard on the telephone line by the caller while the phone they are calling is being rung. It is normally a repeated tone, designed to assure the calling party that the called party's line is ringing, although the ring-back tone may be out of sync with the ringing signal.		White - Comments Solicited			
Supplementary Service Management	A.7.2.5.1.4	The IMS multimedia Telephony communication service consists of two principal parts: a basic communication part, and an optional supplementary services part. The later part of the IMS multimedia telephony communication service consists of a number of specified supplementary services. These are fully standardized to ensure interoperability between multiple end points, and between end points and network control entities. Supplementary services uses SIP as enabling protocol.		White - Comments Solicited			
Directory Assistance Service Management	A.7.2.5.1.4.1	Directory assistance or directory enquiries is a phone service used to find out a specific telephone number and/or address of a residence, business, or government entity.		White - Comments Solicited			
Call Waiting Service Management	A.7.2.5.1.4.2	Call waiting is a feature on the NPSBN. If a calling party places a call to a called party which is otherwise engaged, and the called party has the call waiting feature enabled, the called party is able to suspend the current telephone call and switch to the new incoming call, and can then negotiate with the new or the current caller an appropriate time to ring back.		White - Comments Solicited			
Caller ID Service Management	A.7.2.5.1.4.3	The NPSBN shall support the transmission of telephony caller addressing information (e.g., "Caller ID"). On a per-user basis, the NPSBN SHALL provide the ability to enable or disable the transmission of caller addressing information (e.g., "Caller ID").		White - Comments Solicited			
9-1-1 Services Product Management	A.7.2.5.2	9-1-1 is the emergency telephone number for the North American Numbering Plan (NANP). This number is intended for use in emergency services only. Dialing "9-1-1" from any telephone will link the caller to an emergency dispatch center—called a PSAP, or Public Safety Answering Point—which can send emergency responders to the caller's location in an emergency.		White - Comments Solicited			

E9-1-1 Service Management	A.7.2.5.2.1	In approximately 96 percent of the US, the Enhanced 911 system automatically pairs caller numbers with a physical address. 9-1-1 is the emergency telephone number for the North American Numbering Plan (NANP). This number is intended for use in emergency services only. Dialing "9-1-1" from any telephone will link the caller to an emergency dispatch center—called a PSAP, or Public Safety Answering Point—which can send emergency responders to the caller's location in an emergency.		White - Comments Solicited		
Text To 9-1-1 Service Management	A.7.2.5.2.1.1	In addition to calling 9-1-1 from a phone, NG9-1-1 can enable the public to transmit text, images, video and data to the 9-1-1 center (referred to as a Public Safety Answering Point, or PSAP). Text to 9-1-1 is part of the NG 9-1-1 capability.		White - Comments Solicited		
Provide Connection for NextGen 9-1-1 Service Management	A.7.2.5.2.2	Next-Generation 9-1-1 (NG9-1-1) uses IP technology to initiate emergency sessions via a number of means, including telephony and messaging. A variety of content (i.e., user media, such as video clips and pictures) can also be provided to the NG9-1-1 PSAP. Appropriate NG9-1-1 content can be delivered to dispatchers from the PSAP call-taker		White - Comments Solicited		
Security Requirements Management	A.7.3	Management of security procedures and requirements for the network, applications and devices. Requirements are derived, updated and maintained by leveraging industry best practices, inputs received from FirstNet, federal and state agencies, and industry leaders.		White - Comments Solicited		
Public Safety Product, Feature Roadmap Development	A.7.4	Based on the requirements from Outreach, Sales related to new features and functions on Public Safety for the Local Agency - FirstNet shall work with the provider(s), OEM's on developing and assessing their product portfolio roadmaps associated with each device and network technology to enable the supply of product, features and functionality to meet the agency outreach requirements.	Q-APP-7	Green - FirstNet Only		
Product Management Support for FirstNet Industry Efforts	A.7.5	Responsible for supporting industry efforts in product development and management.		White - Comments Solicited		
Develop Offers (In Support of Sales)	A.7.6	Responsible for developing special product/service/pricing offers.		White - Comments Solicited		
Develop Offers for Proposals	A.7.6.1	Responsible for developing responses to RFPs and other special offers/responses.		White - Comments Solicited		
Approve Offers for Proposals	A.7.6.2	Responsible for reviewing and approving special product/service/pricing offers	Q-BUS-4	White - Comments Solicited		
Stakeholder Management and Marketing	A.8	Functions support overall engagement with key stakeholders that shape the FirstNet network user needs. FirstNet maintains ownership over engaging the stakeholder community, collecting their input and developing requests for the provider(s).	Q-BUS-1, 5	White - Comments Solicited		
Marketing Strategy	A.8.1	Strategy (relative to consultation and marketing) addresses the key elements FirstNet must consider to maintain and grow the user base. This involves understanding of the evolving user experience, the technology required to deliver the optimal features and functionality, and how to balance these needs with the limitations of the business.		White - Comments Solicited		
Planning of the Marketing Strategy	A.8.1.1	Planning represents the implementation of the strategy to maintain and grow the user base. Planning involves and influences most if not all sections of "consultation and marketing".		White - Comments Solicited		
Conducting Market Research	A.8.1.2	Market research involves the understanding of the user experience (both in opt-in and opt-out markets), along with competitive commercial solutions and the evolving technologies, applications, and solutions available to deliver public safety communications services.		White - Comments Solicited		
Defining Pricing Strategy	A.8.1.3	Definition of tariff plans to accommodate all public safety needs.		White - Comments Solicited		
Agreement with Provider(s) on Pricing Strategy	A.8.1.3.1	FirstNet negotiation and agreement with contractor(s) on pricing strategies for services, features and devices based on FirstNet recommended pricing strategy.		Green - FirstNet Only		
Recommendation of Pricing Strategy	A.8.1.3.2	Develops and recommends Pricing Strategy including tariff plans across all services, features and functionality to meet the FirstNet business objectives.		White - Comments Solicited		

Definition of Near Term Public Safety Product Roadmap	A.8.1.4	Develop strategic guidance internal to FirstNet, with our business provider(s), and the public safety stakeholders. This will result in FirstNet being able to provide a plan to shape and define their product's vision.		White - Comments Solicited			
Communications Strategy	A.8.2	Communications represents the outward facing elements at FirstNet responsible to inform government, state, and local agency users and constituents of network status, performance and plans.		White - Comments Solicited			
Public Affairs Communications Strategy	A.8.2.1	Public affairs strategy represents FirstNet's interests within the local, State, and Federal Government constituents. Communications are mostly proactive, trying to anticipate the needs and concerns. However, the function must also support communications on network issues and failures if and when they occur.		Green - FirstNet Only			
Branding & Product Positioning Strategy	A.8.2.2	Branding strategy represents the materials and communications methods used to make FirstNet products and services visible and relevant to the end user. This function must address network services along with evolving technology and applications.		White - Comments Solicited			
Media Strategy Support	A.8.2.3	Media strategy as used in the advertising or content delivery industries, is concerned with how messages will be delivered to First Responders, Agencies, and Secondary users.		White - Comments Solicited			
Social Media Strategy Support	A.8.2.4	Social Media strategy as used in the advertising or content delivery over social media platforms to First Responders, Agencies, and Secondary users.		White - Comments Solicited			
Advertising & Promotion Strategy Support	A.8.2.5	Advertising & Promotion Strategy is the plan to used for attracting and sustaining the First Responder User base.		White - Comments Solicited			
Community Relations Support	A.8.2.6	Support FirstNet in working with local communities to promote public safety communications, including event sponsorships, public awareness drives, etc.		White - Comments Solicited			
Event Communications Support	A.8.2.7	Support FirstNet on the pre and post event media communications as well as media communications during events that involve public safety services including for disasters and other public events (protests, sports, etc.)		White - Comments Solicited			
Market Analysis	A.8.3	This contractor(s) function under Consultation and Marketing will segment FirstNet user populations, analyze each segments needs and requirements and forecast growth and current and new segments.		White - Comments Solicited			
Segmentation Planning	A.8.3.1	This contractor(s) function under Market Analysis will analyze agency segmentations (fire, police, ambulance) by size, state, tribal area and function with respect to their FirstNet requirements.		White - Comments Solicited			
Customer Needs Analysis	A.8.3.2	Media strategy as used in the advertising or content delivery industries, is concerned with how messages will be delivered to First Responders, Agencies, and Secondary users.		White - Comments Solicited			
User Forecasting & Reporting	A.8.3.3	This contractor(s) function under Market Analysis will forecast agency segments (fire, police, ambulance) by size, state, tribal area and function with respect to their FirstNet requirements.		White - Comments Solicited			
PSAC Engagement	A.8.4	PSAC Engagement involves meeting planning and execution and administrative services of the PSAC, its subcommittees, and working group.		Green - FirstNet Only			
Consultation	A.8.5	Engaging and understanding the needs requirements of public safety users through outreach, education and planning. FirstNet owns the role of engaging stakeholders to collect their inputs, balance their needs and define on-going development and network deployment priorities.		White - Comments Solicited			
State/Federal/Tribal Consultation	A.8.5.1	Process with regional, state, tribal and local jurisdictions regarding the development of State/Territory plans for building, operating, and deploying the network. This function will also support related consultation with federal agencies.		White - Comments Solicited			
Support Consultation Efforts	A.8.5.1.1	Provide technical expertise and operational support for engaging stakeholders during FirstNet led consultation events and conferences. This includes providing technical and design materials to engage conversations around network design, functionality and the identification, tracking and resolution of stakeholder needs		White - Comments Solicited			

Facilitate Resolution of Issues	A.8.5.1.2	Coordinating stakeholder input and needs with the provider(s) to come to resolution on user and technical issues.		Green - FirstNet Only			
State/Federal/Tribal Outreach	A.8.5.1.4	Educating public safety and other stakeholders at the federal, state, tribal, and local levels about FirstNet technology, the vision for the network, and the process to build out the network. FirstNet will engage stakeholders in a comprehensive, long-term, two-way dialogue to ensure the system once implemented will continue to meet their needs, addresses their challenges and concerns, and encourages them to actively participate. Outreach will also help ensure the states have what they need for their internal outreach to the state, county, local, and tribal levels. Engagements will also direct and identify markets and key target areas to connect the provider(s) with stakeholders		White - Comments Solicited			
Events Management	A.8.5.1.4.1	Engagement and coordination in support of state, tribal, federal and association conferences, meetings and events. These efforts includes the full array of in-person events, webinars, telephone and video conferencing.		Green - FirstNet Only			
Events Management Support	A.8.5.1.4.2	Conference and event planning support required for various FirstNet functions held throughout the contract. Conference planning should include the entire spectrum of event planning and conference management, as well as a customized, targeted approach to ensure that each conference or event is successful.		White - Comments Solicited			
State Plan Development	A.8.5.2	Working closely with Consultation staff as well as the technical design staff to ensure that the state desires are considered and reflected in the individual state plans. State plans will integrate the network design, consultation and business plan outputs into a document that each state will review to make its opt-in/opt-out decision. The individual state plans will include information about our terms and conditions, expectations, legal requirements, provider(s)ship information, legal user definition and associated fees, network topology, and coverage goals. Plans will also include state specific information about the radio access network (RAN) design and evolved pack core (EPC) design, including but not limited to coverage goals, implementation methodology and timeline, proposed tower locations, and total investment by FirstNet in the state.	Q-BUS-5	White - Comments Solicited			

Pre State Plan Development Support	A.8.5.2.1	Provide FirstNet State Plans team with subject matter experts (SME), technical writers, graphic designers to support the collection of data, development of products, meeting materials and oral presentations in the drafting and development of the 56 state and territorial plans. Products include but are not limited to the Following: <ul style="list-style-type: none"> • State Radio Access Network Plan • State Coverage Summary Plan • Environmental Factors Report • Service level Agreements • Reliability and Resiliency Plan • Security Plan • FirstNet National/Regional Design Plan • Network Deployment Plan • Device and Applications Plan • Network Operations Plan • Financial Plan 		White - Comments Solicited			
Post State Plan Support	A.8.5.2.2	Provide FirstNet State Plans team with subject matter experts (SME), technical writers, graphic designers to support continued coverage and user needs identified post state plan development.		White - Comments Solicited			
Public Safety Stakeholder Data Collection & Analysis	A.8.5.2.3	Defines, collects and analyzes state needed data elements around areas such as coverage objectives, user and operational areas, capacity planning, current and training needs for incorporation into the state planning function.		Green - FirstNet Only			
State Plan Change Management	A.8.5.2.4	Coordinates stakeholder inputs, requests and engagements relative to changes during the planning, IOC and FOC phase		Green - FirstNet Only			
State Plan Delivery to Governor	A.8.5.2.5	Consolidate state consultation/outreach data with provider(s) provided support products into a final state plan for signature by the governor.		Green - FirstNet Only			
Governmental Affairs	A.8.5.3	Interface and consultation with appropriate governmental entities regarding FirstNet.		Green - FirstNet Only			
Direct Interaction with Congress	A.8.5.3.1	Direct interaction with members of Congress and their staff.		Green - FirstNet Only			
Development Federal/Congressional Outreach Plans	A.8.5.3.2	Develop and implement the outreach plan for federal and congressional interaction.		Green - FirstNet Only			
Communication with Relevant Jurisdiction Committees	A.8.5.3.3	Working with the relevant committees of jurisdiction.		Green - FirstNet Only			
Communication Development Across Federal Government	A.8.5.3.4	Coordinating messaging and message development across the federal government.		Green - FirstNet Only			
Develop Hearing Testimonies	A.8.5.3.5	Develop hearing testimony and information for congressional hearings and roundtables.		Green - FirstNet Only			
Support States on FirstNet Related Items	A.8.5.3.6	Direct interaction with state governments including the executive and legislative branches.		Green - FirstNet Only			
Support Local Governments on FirstNet related items	A.8.5.3.8	Work with city mayors, town councils, and other forms of local government on FirstNet related issues.		Green - FirstNet Only			
User Fee Administration	A.8.6	Manages user rate plan definitions and associated user fees.		White - Comments Solicited			
User Fee Determination with Contractor(s)	A.8.6.1	Provides the venue to come to a mutual agreement on what the reoccurring fees would be to access the network for each user.		White - Comments Solicited			
User Fee Implementation	A.8.6.2	Execution of all marketing collateral (e.g. website, flyers, etc.) regarding the user fee structure agreed with FirstNet.		White - Comments Solicited			
User Fee Approval Process Management with NTIA	A.8.6.3	Formulating and providing recommendations for fees assessed with network user fees, lease fees related to network capacity and lease fees related to network equipment and infrastructure.		Green - FirstNet Only			
Definition of Device Portfolio	A.8.7	Responsible for commercial discussions and negotiating with device and embedded application provider(s) to define and build a portfolio of devices.	Q-DEV-1	White - Comments Solicited			
Commercial Discussions/Negotiations for Devices & Pricing	A.8.7.1	Commercial discussions and negotiations for FirstNet devices including information gathering, initial proposal and negotiation, and proposal modifications to final contract.		White - Comments Solicited			

