

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
White - Comments Solicited	A.2	Life Cycle Management	Overall oversight and management of the life cycle of NPSBN services including user management, supply chain management and technical execution
	A.2.1	User Management	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.
	A.2.1.1	User Security Administration	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.
	A.2.1.1.1	User Fraud Management	Enacting processes and procedures to detect and prevent fraud in regard to accounts, devices, applications, and sharing of sensitive data.
	A.2.1.2	Customer Service Process Development	Develop and implement processes and systems for a helpdesk capability for state and agency users.
	A.2.1.2.1	Customer Service For Tier 2+ Support	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.
	A.2.1.2.3	Provide Tier 1 type Troubleshooting Public Safety Entity support	Provide Tier 1 customer service/technical support to public safety users.
	A.2.1.3	Public Safety Entity Management	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.
	A.2.1.3.1	Device Administration	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.
	A.2.1.3.1.1	Hardware Management	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.
	A.2.1.3.1.1.1	IMEI/UICC Inventory Management	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 policies 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.
	A.2.1.3.1.1.3	Manage, Stock, & Distribution of Hardware	Contractor(s) to order and return devices and device accessories through online and other systems supported by contractor(s)' device procurement process.
	A.2.1.3.1.3	Over The Air (OTA) Management	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.
	A.2.1.3.3.1.2.3.1	Communications Groups Deactivation	Allows an agency to turn off the user or devices assignments to communications groups.
	A.2.1.3.3.1.3	Provisioning of Users	Allows an agency to provision a user or device on the NPSBN and allows it to administer profiles, services, group subscriptions for the user.
	A.2.1.3.3.1.3.1	User Profile Assignment	Allows an agency to assign the user to an active profile that has already been provisioned appropriately.
	A.2.1.3.3.1.3.2	Rating (Billing) Activation	Allows the agency to assign the appropriate billing for the individual user or device.
	A.2.1.3.3.1.3.3	Installation of Services & Applications	Allows an agency the ability for specific local applications to be installed on devices or specific services be activated.
	A.2.1.3.3.1.3.3.1	Communications Groups Implementation	Allows an agency to assign the user or devices to appropriate communications groups.
	A.2.1.4	Agency/State Network Monitoring	Monitoring the network operational status and the status of associated repair or reconfiguration steps in their respective area for agencies.
	A.2.1.4.2	Critical Outage Notification to Dispatch Center	Monitoring the status of outages and reporting that status to dispatch centers.
	A.2.1.5	End User Training	Support the training of users in network and device usage for the local public safety agencies and/or state jurisdictions
	A.2.1.5.2	Training on FirstNet Hosted Apps and Network Services	Training agencies on how to use FirstNet approved devices and FirstNet applications, as well as FirstNet network usage.
	A.2.1.6	Manage Individually Liable Accounts	Provide user account services for individually liable accounts
	A.2.1.6.1	Provide Verification Services and User Provisioning	Provide verification and provisioning for individually liable accounts
	A.2.1.6.2	Support User Purchasing	Provide user purchasing processes for individually liable accounts

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.2.1.6.3	Provide Tier 1 Support	Provide Tier 1 customer service/technical support for individually liable accounts
	A.2.1.7	Service Quality Evaluation from PS User Perspective and Improvement Activities	Contractor(s) to perform the monitoring, assessment, and improvement of public safety user experiences, utilizing both subjective and objective methodologies.
	A.2.2	Supply Chain Management	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
	A.2.3.1	Technical Project Management	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.
	A.2.3.1.1	Technical Schedule & Risk Management	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.
	A.2.3.1.2	Engineering & Integration Risk Management	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.
	A.2.3.3	Technical Strategy	Development of long and short range roadmaps and strategy for the NPSBN.
	A.2.3.5	Supply Chain Management Oversight	Oversight of all supply chain issues relating to systems engineering lifecycle activities.
	A.3	Engineering & Network Operations	This function represent the activities required in designing and maintaining the operation of a wireless network.
	A.3.1	Network Financial Administration	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.
	A.3.1.1	Network CAPEX/OPEX Forecasting	Function reviews expenditure trends to monitor network projects and meet approved budgets. The function also supports planning of future expenditures.
	A.3.1.2	Network Financial Control	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.
	A.3.1.3	Business Case Development/Analysis	Provides the management team a detailed business case analysis of the feasibility network-related services.
	A.3.1.4	Actual Network Spend Reporting	Produce report on variances between actual expenditures and approved spending levels, both operating and capital expense.
	A.3.2	Network Deployment	Network deployment represents the services and functions required to initially enable, and to continually manage growth and expansion of PSBN network services and functionality.
	A.3.2.1	Installation of Network Elements	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.
	A.3.2.2	Transmission Network Installation	End-to-end transport connectivity of each network element and verification of circuit capacity and performance (per associated acceptance tests and verification punch lists).
	A.3.2.3	Site Acquisition Secure & Preparation	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.
	A.3.2.4	Warehousing/Inventory (Fixed Asset Management)	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.
	A.3.3	Priority & QoS Administration	The administration of all priority and QoS policy frameworks for the NPSBN.
	A.3.3.1	Profile Configuration Setup	Setup and configure parameters of user QoS and priority profiles for different services and applications in the NPSBN.
	A.3.3.2	Implement Profile Changes	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.
	A.3.3.3	Drive Supplier Roadmap for QPP	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.
	A.3.4	Engineering & Planning	Function serves planning to evolve the network elements, features, and services to meet future needs of First Responders.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.4.1	Long Term Feature Planning	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.
	A.3.4.1.1	Proof of Concept & Field Testing	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.
	A.3.4.1.1.1	Research/Prototype Testing	Researching and prototyping new technology, services and features to determine the viability for deployment within FirstNet to meet the needs of public safety users.
	A.3.4.1.1.2	Interworking Proof of Concept & Field Trials	Prototype interworking and field trials of new devices, technologies, services and features within the current FirstNet infrastructure.
	A.3.4.1.1.3	Prototype Device Testing	Testing new prototype devices and determine potential uses and functional value for implementation within FirstNet.
	A.3.4.1.1.4	Prototype RAN Feature Testing	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.
	A.3.4.1.1.5	Prototype Services Testing	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.
	A.3.4.1.2	Long Term Product Management	Develop three year+ public safety product roadmap to drive industry and standards development.
	A.3.4.1.2.1	Customer Feedback for Long Term Services	Customer feedback and requirements gathering for development of three year+ and beyond public safety product roadmap.
	A.3.4.1.3	Long Term Feature Feasibility Analysis	Proof of Concept Analysis provides feasibility analysis for feature planning. This function will access the financial and technical feasibility of the new offered or required feature or function for FirstNet.
	A.3.4.1.4	Supplier Roadmap Coordination	This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.
	A.3.4.2	Network Design & Architecture	Design and architect a cost effective and optimal NPSBN.
	A.3.4.2.1.1	Local Control User Service Admin Development & Maintenance	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.
	A.3.4.2.1.2	Development of Local Control User Operations Guideline	Develops guideline to support network monitoring, provisioning, QPP provisioning, and accounting.
	A.3.4.2.1.2.1	Operations Guideline for Static & Dynamic Profiles	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.
	A.3.4.2.1.2.2	Operations Guideline for NIMS ICS	The contractor(s) shall follow and implement the policy, governance guidelines of national incident management with FirstNet and other federal/local agencies.
	A.3.4.2.1.2.2.1	NIMS ICS Type 3,4 & 5 Local Control Process	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.
	A.3.4.2.1.2.2.2	NIMS ICS Type 1 & 2 Local Control Process	Manage the adoption and ongoing compliance of existing NIMS ICS Types 1 & 2 protocols and processes within the local control capabilities in the NPSBN.
	A.3.4.2.2.1	Mission Critical PTT (3GPP) Engineering	Engineer and design mission critical push to talk services as defined by product management.
	A.3.4.2.2.2	Group Communications Engineering	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.
	A.3.4.2.2.4	Location Platform Engineering	Plan, design and engineer Location technology solutions for the NPSBN to enable true location awareness for public safety users and devices.
	A.3.4.2.2.5	IMS Platform Engineering	Plan, architect, design and engineer the IP Multimedia Subsystem (IMS), to support the delivery of IP multimedia services such as VoLTE, Identify Management etc..
	A.3.4.2.2.5.1	VoLTE Engineering & Design	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.
	A.3.4.2.2.5.2	Other IMS Services Engineering & Design	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.
	A.3.4.2.2.5.3	Presence Engineering & Design	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.4.2.2.5.4	IP Messaging Engineering & Design	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.
	A.3.4.2.2.6	Broadcast Platform Engineering	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.
	A.3.4.2.2.7	Designing and Engineering Mobile Device Management Systems	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.
	A.3.4.2.2.7.1	Designing and Engineering Support for Multi-Tenant Management	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.
	A.3.4.2.2.7.10	Designing and Engineering Systems for Mobility Management	Plan and design the device management functionality required to support sending of mobility management related updates to mobile devices.
	A.3.4.2.2.7.2	Designing and Engineering Support for Policy & Content Management	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.
	A.3.4.2.2.7.3	Designing and Engineering Support for Over The Air (OTA) Updates	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.
	A.3.4.2.2.7.4	Designing and Engineering Mobile Diagnostics, Polling, & Reporting Tools	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.
	A.3.4.2.2.7.5	Designing and Engineering Software, OS, & Firmware Management Tools and Processes	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.
	A.3.4.2.2.7.6	Designing and Engineering Support for Tethered Device Updates	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".
	A.3.4.2.2.7.7	Designing and Engineering Configuration Management Tools and Systems	Develop, plan, architect and design device configuration management. This includes the capability of polling & updating all devices in the FirstNet device portfolio.
	A.3.4.2.2.7.8	Designing and Engineering Enabling Tools and Methods for BYOD Users	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.
	A.3.4.2.2.7.9	Designing and Engineering for UICC/SIM Management	Plan and design UICC profiles for network configurations, roaming provider(s) and other necessary applications.
	A.3.4.2.2.8	ProSe Engineering & Design	Plan and design proximity services using LTE technologies to connect mobiles for direct communications.
	A.3.4.2.2.8.1	Direct Mode Communications Engineering	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.
	A.3.4.2.2.8.2	Discovery Systems Engineering	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.
	A.3.4.2.3	Transmission Systems Management	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.
	A.3.4.2.3.1	Transmission Systems Ordering	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.4.2.3.2	Transmission Systems Forecasting	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.
	A.3.4.2.3.3	Transmission Systems Design	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.
	A.3.4.2.4	Core Network Design	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.
	A.3.4.2.4.1	Core Architecture Design	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.
	A.3.4.2.4.2	Capacity Planning	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.
	A.3.4.2.4.3	Core Software License Management	Manage all core software licenses for all EPC equipment as well all other core peripheral equipment
	A.3.4.2.5	Traffic Management	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.
	A.3.4.2.5.1	Traffic Monitoring & Reporting	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.
	A.3.4.2.5.2	Traffic Forecasting	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.
	A.3.4.2.6	Radio Network Design	Provides eNodeB planning to address coverage and capacity requirements. Creating solutions based on available hardware/software options with optimal location for sites and antennas.
	A.3.4.2.6.1	RAN License Management	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.
	A.3.4.2.6.2	RAN Coverage Engineering	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.
	A.3.4.2.6.3	Deployables Engineering	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.
	A.3.4.2.6.4	RAN Capacity Engineering	Design capacity solutions to address sites which are overloaded to meet performance requirements from the air interface perspective.
	A.3.4.2.6.5	RAN Integration of Rural Carriers, Other Provider(s) networks, Opt-out States for Boundary Areas	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.
	A.3.4.2.7	Application Platform Design	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.
	A.3.4.2.7.1	Mobile Application Development Platform Design	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.4.2.7.1.1	Developer Portal Design	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.
	A.3.4.2.7.1.2	Mobile Application Framework Design	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.
	A.3.4.2.7.1.3	Develop SDKs and Development Tools	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.
	A.3.4.2.7.1.4	Develop Application Test Platform	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
	A.3.4.2.7.2	Design App Store	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.
	A.3.4.2.7.3	Design Service Delivery Platform Development	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.
	A.3.4.2.7.3.1	South Facing API Implementation	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.
	A.3.4.2.7.3.2	North Facing API Implementation	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.
	A.3.4.2.8	System Hardening Design	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.
	A.3.4.2.8.1	Reliability Design	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.
	A.3.4.2.8.2	Resiliency Design	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.
	A.3.4.2.8.3	Disaster Recovery Planning/Design	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.
	A.3.4.2.9	Provide Cloud Services Administration	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.4.2.9.1	Develop and Manage Agency Information Homepage	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.
	A.3.4.2.9.2	Develop and Manage Application Hosting	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.
	A.3.4.2.9.3	Develop and Manage Cloud Services	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.
	A.3.4.2.9.4	Develop BigData Analytic Platform and Associated Services	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.
	A.3.4.3	End to End NPSBN Architecture Definition	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.
	A.3.5	Business Support Systems (BSS) Management	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.
	A.3.5.1	Local Control: Service & User Provisioning	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.
	A.3.5.2	Billing Administration	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.
	A.3.5.2.1	Billing Reporting	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.
	A.3.5.2.1.1	Usage Reporting	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.
	A.3.5.2.1.2	Billing Data Analytics	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.
	A.3.5.2.2	Revenue Assurance (Fraud Management)	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.).
	A.3.5.2.3	Roaming Billing Administration	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.
	A.3.5.2.4	Opt Out State Billing Administration	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.
	A.3.5.2.5	Secondary Usage via CLA Billing Administration	Provide systems capability and services to administer user billing for secondary users. Maintain detailed records of CDRs and other billing records for historical review.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.5.2.6	Invoicing & Billing	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.
	A.3.5.2.7	Rating & Pricing	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.
	A.3.5.3	Business Intelligence	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.
	A.3.5.3.1	User Business Intelligence Data Analytics	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.
	A.3.5.4	Billing Systems Maintenance	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.
	A.3.5.4.1	Define Billing Profiles	Define standard and custom user, service, application, and device profiles for use in rate plans and other billing administration services.
	A.3.5.4.2	Mediation Platform Administration	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.
	A.3.5.4.3	Billing Software Updates	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.
	A.3.5.4.4	Billing System Reporting	Develop and maintain administration servers, remote desktop user interface and control systems for Billing Administrators to generate various reporting on billing functions.
	A.3.5.4.4.1	Billing Intelligence Data Analytics	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.
	A.3.5.4.4.2	System Usage Reporting	Develop and maintain servers, remote desktop user interface, and control systems for "self-service" Usage Reporting capabilities to be performed by FirstNet and PSEs.
	A.3.5.5	Customer Relationship Management (CRM)	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.
	A.3.5.6	Data Storage Administration	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.
	A.3.6	Performance Management	Provides the capabilities to optimize the user performance and experience of the overall NPSBN.
	A.3.6.1	Service Optimization	Optimize the performance of services to based on the review and analysis of relevant network performance, customer service feedback and trends.
	A.3.6.2	Parameter Standardization	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
	A.3.6.3	Network Optimization	Network optimization to meet QASP KPIs and network guidelines using outage mitigation, coverage tuning, capacity tuning, configuration optimization and coverage field testing and measurement.
	A.3.6.3.1	Outage Mitigation	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
	A.3.6.3.2	Coverage Tuning	Measure radio performance in the field using appropriate methods and optimize radio parameters to improve the quality of radio coverage.
	A.3.6.3.3	Capacity Tuning	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
	A.3.6.3.4	Configuration Optimization	Monitor network performance in the core and radio networks and optimize network configuration for improved performance, quality and reliability for public safety

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.6.3.5	Coverage Field Testing & Measurement	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
	A.3.6.4	KPI Monitoring	Monitoring and development all necessary QASP reporting to FirstNet in compliance with contractual requirements.
	A.3.7	O&M Interfaces & Tools	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.
	A.3.7.1	Data Storage for Tools Administration	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.
	A.3.7.2	Field Measurement Tool Management	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.
	A.3.7.3	Element Management System Administration	Support element management systems for upgrades and troubleshoot failures. Provide or revoke user access to such systems. Maintain database backups of network configuration.
	A.3.7.4	KPI Development	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.
	A.3.7.5	KPI Reporting	Design and distribution of network performance and status reports throughout the organization. Build customized reports based on input from various functional teams.
	A.3.7.5.1	Network Events & Alerting Administration	Reporting of network outages or errors for alerting network engineers to address immediately. Severity levels of incident can be created based on network impact.
	A.3.8	Network Management	The network management function supports the major operational related items for maintaining network performance. Ensuring all elements of the network are functioning appropriately.
	A.3.8.2	Operations & Maintenance	Performing all aspects related to efficient operations of the NPSBN, including all ITIL functions around service support and on-going service delivery.
	A.3.8.2.1	Experience Center & Training Creation and Management	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
	A.3.8.2.1.1	Public Safety ICS Training	Development of network training programs to support of ICS communications staff for incident and event communication management.
	A.3.8.2.1.2	NPSBN feature demonstrations	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.
	A.3.8.2.1.3	Implementation & Updates Management	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).
	A.3.8.2.2	Network Maintenance	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.
	A.3.8.2.2.1	Hardware & Software Updates	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.
	A.3.8.2.2.2	Equipment or Service Repair	Repair includes physical (hardware or facility replacement/repair) and software/translation related modifications required to restore service to full user functionality.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.8.2.2.3	Equipment Spares Management	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.
	A.3.8.2.2.4	Preventative Maintenance	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.
	A.3.8.2.3	Operations	The operations function serves to manage the configuration, optimization, and implementation of the network elements.
	A.3.8.2.3.1	Network Configuration Management	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.
	A.3.8.2.3.1.1	Roaming Configuration Management	Manage the configuration of each NPSBN node to support and provide the designed roaming functionality and features.
	A.3.8.2.3.1.2	Network Identifier Management	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.
	A.3.8.2.3.1.3	Managing Network Settings For Mobile Devices	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.
	A.3.8.2.3.2	Lawful Intercept Management (CALEA)	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.
	A.3.8.2.3.2.1	Other Services Intercept Authorization & Execution (e.g. location)	Manage the authorization and execution of Other services intercept with Law Enforcement Agency in providing the "suspect(s)" location (CellID, Lat, Lon) etc.
	A.3.8.2.3.2.2	Cyber Monitoring Authorization & Execution	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.
	A.3.8.2.3.2.3	Signaling Intercept Authorization & Execution	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.
	A.3.8.2.3.2.4	Voice Intercept Authorization & Execution	Manage the authorization and execution of Voice intercept with the Law Enforcement Agency in providing the suspect(s) Voice traffic in real-time.
	A.3.8.2.3.2.5	Data Intercept Authorization & Execution	Manage the authorization and execution of Data intercept with the Law Enforcement Agency in providing the suspect(s) Data traffic in real-time.
	A.3.8.2.3.2.6	Messaging Intercept (SMS/MMS) Authorization & Execution	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.
	A.3.8.2.3.3	Release Management	Managing new software and hardware updates (minor and major releases) across the NPSBN.
	A.3.8.2.3.3.1	New or Upgrade Network Elements Release Management	Managing hardware updates across the NPSBN as required to support the product management roadmap, enhanced functionalities, and capacity needs.
	A.3.8.2.3.3.2	New or Upgrade Software Release Management	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.
	A.3.8.2.3.3.3	New or Upgrade Feature or Functionality Release Management	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.
	A.3.8.2.3.4	Device Management Systems Operations	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.8.2.3.4.1	Operating the Multi-Tenant Management Access and Permissions	Manage access system permissions for agency administrators to the device management system.
	A.3.8.2.3.4.10	Operating Mobility Management for Devices	Utilize the device manager to control and provide updates to devices in regards to mobility management such as roaming provider(s) and prioritization.
	A.3.8.2.3.4.2	Operating Device Policies & Content Management	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.
	A.3.8.2.3.4.3	Management of Over The Air (OTA) Updates	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.
	A.3.8.2.3.4.4	Managing Tools for Diagnostics, Polling, & Reporting on the Device	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.
	A.3.8.2.3.4.5	Mobile Device Software, OS, & Firmware Management	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.
	A.3.8.2.3.4.6	Updating Mobile Device Via Tethering Arrangements	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".
	A.3.8.2.3.4.7	Operating and Maintaining Mobile Device Configuration Management	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.
	A.3.8.2.3.4.8	Updating and Tracking Mobile Devices for BYOD Users	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.
	A.3.8.2.3.4.9	Providing UICC/SIM Management for Devices	Utilize the device management function to set and update UICC configurations and applications.
	A.3.8.2.3.5	Network Impairment Triage	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.
	A.3.8.2.3.5.1	After Action Reporting	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.
	A.3.8.2.3.5.2	Tier 1 Support	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.
	A.3.8.2.3.5.3	Tier 2 Support	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.
	A.3.8.2.3.5.4	Tier 3 Support	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).
	A.3.8.2.3.6	Problem Management	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.
	A.3.8.2.3.6.1	Problem Investigation & Resolution	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.
	A.3.8.2.3.6.2	Continual Service Improvement	Continual service improvements are the review of recommendations and implementation across all services for applicability to reduce further risk of problem reoccurrence.
	A.3.8.2.4	Quality Assurance & Testing	Perform the overall testing for all devices to ensure compatibility and performance specifications are met on the network.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.8.2.4.1	Designing and Carrying out Mobile Device Carrier Acceptance Test Plans and Approvals	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.
	A.3.8.2.4.1.3	Device Performance Testing	This function specifically calls out the testing of device performance, including RF, mobility and similar quality features.
	A.3.8.2.4.1.3.2	Device Interoperability Testing	Testing of features and functionality interoperating with other devices and systems.
	A.3.8.2.4.1.3.5	Application Interoperability Testing	Testing device application Interoperability ensuring device applications meet performance requirements.
	A.3.8.2.4.1.4	User Equipment Certification	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.
	A.3.8.2.4.1.4.1	Conduct FCC Type Certification	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.
	A.3.8.2.4.1.5	Device Administration of Secondary User via CLA	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).
	A.3.8.2.4.2	Field Testing	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.
	A.3.8.2.4.2.1	Major Software/Hardware Upgrade Testing	Testing of new software and hardware updates (minor and major releases) across the NPSBN.
	A.3.8.2.4.2.2	New Services Testing	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).
	A.3.8.2.4.3	Interconnection Testing	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.
	A.3.8.2.4.3.1	S1 Interconnection Testing (Opt-out RAN)	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.
	A.3.8.2.4.3.2	ISP/PSTN Interconnection Testing	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.
	A.3.8.2.4.3.3	Roaming Interconnection Testing	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.
	A.3.8.2.4.3.4	Inter-carriers Interconnection Testing	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.
	A.3.8.2.4.3.4.1	WiFi Interconnection Testing	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.
	A.3.8.2.4.3.5	Backhaul & Backbone Interconnection Testing	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).
	A.3.8.2.4.3.6	PSEN Interconnection Testing	Testing connections and routing between NPSBN and the PSENs to validate APN connections to PSEN and mobile VPNs.
	A.3.8.2.4.3.7	Cloud Services Interconnection Testing	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.8.2.4.4	Application Certification	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.
	A.3.8.2.4.4.1	3rd Party Sandbox Certification	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.
	A.3.8.2.4.4.2	FirstNet Hosted Application Certification	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.
	A.3.8.2.4.5	Configuration Testing	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.
	A.3.8.2.4.5.1	Device Manager Platform Testing	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.
	A.3.8.2.4.5.2	RAN Equipment Testing	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.
	A.3.8.2.4.5.3	Core Network Equipment Testing	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.
	A.3.8.2.4.5.4	Application Delivery Platform Testing	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.
	A.3.8.2.4.6	Service Experience Management	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.
	A.3.8.2.4.6.1	Service Experience Data Analytics	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.
	A.3.8.2.4.6.2	Service Availability Management	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.
	A.3.8.2.4.6.3	Service Capacity Management	Capacity management ensures that services are architected with the capacity to meet current and immediate future business capacity needs.
	A.3.8.2.4.6.4	Service Level Management	Service level management is the identification and monitoring of relevant KPIs to ensure end user quality of service metrics are met or exceeded.
	A.3.8.2.5	Security Systems Management	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.8.2.5.1	Physical Security Management	Manage the physical access to all NPSBN locations according to FirstNet's security policies.
	A.3.8.2.5.2	Personnel Identity Management	Manage the personnel access to all NPSBN locations according to FirstNet's security policies.
	A.3.8.2.5.3	Cyber Security Monitoring	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.
	A.3.8.2.5.3.1	Security Threat Mitigation	Develop procedures, processes, and implement functions in security systems to mitigate against potential security breaches.
	A.3.8.2.5.4	Security Policy Enforcement	FirstNet 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.
	A.3.8.2.6	Disaster Response & Recovery (NIMS Types 1,2,3) & Major Planned Event Operations	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.
	A.3.8.2.6.1	Network Restoration	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
	A.3.8.2.6.2	Disaster response information gathering	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.
	A.3.8.2.6.3	Agency Coordination	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.
	A.3.8.2.6.4	Event Tracking	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.
	A.3.8.2.6.5	Event Preparation	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.
	A.3.8.2.6.5.1	Incident Setup & Management	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.
	A.3.8.2.6.6	Mitigation Plan Development	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.
	A.3.8.2.6.6.1	Mitigation Implementation	Mitigation plans will be implemented as required on-site during events and as part of simulated (training) events.
	A.3.8.2.6.7	Post Incident & Event Analysis Reporting	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.
	A.3.8.3	Network Monitoring	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.
	A.3.8.3.1	National Network Operations Center Management	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.
	A.3.8.3.1.1	Trouble Ticket Management/Coordination	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.
	A.3.8.3.1.2	Management of Network Events	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.3.8.3.2.1	Intrusion Prevention	Prevent security intrusions by proactive and real-time sampling of network traffic and reviewing logs to detect and eliminate in-progress and future threats.
	A.3.8.3.2.2	Intrusion Recovery	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.
	A.3.8.3.2.3	Internal Security Compromise Detection	Detecting threats originating from within the trusted network or system.
	A.3.8.3.2.4	External Security Intrusion Detection	Detecting threats originating from outside the trusted network.
	A.3.8.3.3	Federal Security Operations Center Management	Communications management between the federal security operations center and the NPSBN security center.
	A.3.8.3.4.2	Device Malware Detection and Deletion	Software and monitoring functionality to identify and correct (or isolate) malware located on user devices.
	A.3.9	Field Testing for Public Safety Services	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.
	A.3.9.1	Public Safety Use Case Testing and Verification	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
	A.3.9.2	Public Safety User Experience Assurance & Verification	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
	A.3.9.3	Public Safety Service Quality and Capability Assurance	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
	A.4	Policies and Procedures	Define policies and procedures focused on business processes related to provisioning, billing, certification, profiles, deployment and operational guidelines.
	A.4.1	Define, Monitor, & Implement Provisioning Policies & Procedures	Provide the provisioning policies and procedures relating to subscription management of agencies and users.
	A.4.2	Define, Implement, & Monitor Network Policies & Procedures	Develop, implement, and monitor overall operating policies and procedures for the NPSBN fully compliant with all laws, rules, standards, and regulations, applicable to FirstNet.
	A.4.2.1	Define & Implement Operational Procedures	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.
	A.4.4	Define, Monitor, & Implement Billing Policies & Procedures	Provide the policy and procedures related to billing subscription and their rate plans for both home and roaming scenarios.
	A.4.5	Develop Best Practices	Define best practices for security, industry standards on processes, network and business operations incorporating agency and state key learnings.
	A.4.6	Develop Customer Care Policies & Procedures	Development of policies and procedures related to the support and care of users including account management, resolving user issues, and billing.
	A.4.7	Develop Marketing Policies & Procedures	Developing and managing marketing policies and procedures in consultation with states and agencies.
	A.4.8	Develop Sales Policies & Procedures	Developing and managing sales policies and procedures in consultation with the provider(s) and states.
	A.5	NPSBN Services Program Management & Contract Compliance	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.
	A.5.1	Agency Administration Program Support	Responsible for coordinating with state, federal, tribal, or other agencies for any agency-specific program needs or reporting.
	A.5.2	Services Program Support & Reporting	Responsible for managing a portfolio of services. This includes service roadmap planning, usage reporting, and new service definition.
	A.5.3	Network Operation Program Support	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.
	A.5.4	Contract Financial Administration	Responsible for managing and reporting the financial performance of the network solution contracts, including financial variance reporting, forecasting, and change management.
	A.5.4.1	Revenue Variance Reporting	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.
	A.5.4.2	Cost Variance Reporting	Responsible for the reporting of the difference between budgeted cost of work performed, and the actual cost of work performed.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.5.4.2.1	Cost of Sales Reporting	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.
	A.5.4.2.2	General & Administrative Cost Reporting	Reporting of expenditures related to sales, general and administrative costs.
	A.5.4.3	Contract Performance Tracking	Responsible for tracking the financial performance of the contract for the implementation of the network solutions.
	A.5.5	Regulatory Management	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
	A.5.5.1	Preparation of Regulatory Filings and Forms	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
	A.5.5.2	NBPSN Regulatory Compliance Monitoring & Reporting	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
	A.5.5.3	Reporting of Opt-Out State Compliance	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
	A.5.6	Legal Support	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
	A.5.6.1	Legal Compliance Monitoring & Reporting	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
	A.6	Sales Management	Responsible for working with the provider(s) on the sales strategy and framework for public safety devices and services
	A.6.1	Public Safety Entity Sales Channel Management	Responsible for agreeing with provider(s) on overall sales targets and performance for devices and services
	A.6.1.1	Local Sales	Responsible for working with public safety agencies on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.1.1	Law Enforcement Sales	Responsible for working with law enforcement agencies on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.1.2	Fire Department Sales	Responsible for working with Fire departments on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.1.3	EMS Sales	Responsible for working with Emergency Medical Service agencies on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.1.4	911 Sales	Responsible for working with 911 service centers on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.1.5	Others Entity Sales	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
	A.6.1.2	Federal Sales	Responsible for working with Federal Government departments on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.2.1	Federal Public Safety Sales	Responsible for working with Federal Government public safety departments on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.2.2	Federal Non Public Safety Sales	Responsible for working with Federal Government non-public safety departments on sales, service performance and soliciting inputs on evolving requirements for devices and services
	A.6.1.3	State Government and Tribal Sales	Responsible for working with State Government and Tribal organizations on sales, service performance and soliciting inputs on evolving requirements for devices and services.
	A.6.1.3.1	State Government and Tribal Public Safety Sales	Responsible for sales activities and user acquisition within state government and tribal organizations.
	A.6.1.3.2	State Government and Tribal Non Public Safety Sales	Responsible for sales activities and user acquisition within non public safety of state government and tribal organizations.
	A.6.1.4	Retail Sales	Responsible for sales activities and user acquisition within the retail channel.
	A.6.1.4.1	Retail/Provider(s) Sales	Responsible for sales activities and user acquisition within the retail provider(s) channel.
	A.6.1.4.2	Retail/3rd Party Sales	Responsible for sales activities and user acquisition within the 3rd party retail channel.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.6.1.5	Internet and Telemarketing Sales	Responsible for indirect sales channels and soliciting inputs on evolving requirements for devices and services.
	A.6.1.6	Utility Responder Sales	Responsible for working with private sector sales channels on sales and evolving requirements for devices and services.
	A.6.1.6.1	Sales to Utilities	Responsible for working with utility sales channels on sales and evolving requirements for devices and services.
	A.6.1.7	Account Management	Responsible for the strategy on account management for pre and post sales and marketing.
	A.6.1.7.1	Customer Acquisition Planning & Implementation	Responsible for the strategy on customer acquisition through promotions, sales channels, and collateral.
	A.6.1.7.2	Customer Retention & Winback Planning and Implementation	Responsible for the strategy on customer retention and winback.
	A.6.1.7.3	Account Planning	Development of the strategy for account planning regarding sales and on-going account management.
	A.6.1.7.4	Special Pricing Development	Development of special pricing offers for enterprise.
	A.6.1.8	User Migration and Evolution	Supports the migration of users from existing LMR, public safety private wireless networks, opt-out states networks, and commercial networks to the NPSBN.
	A.6.2	Sales Operations & Support	Responsible for developing the framework together with the provider(s) for an efficient sales operation and support service
	A.6.2.1	Sales Reporting	Monitor and produce high level management reports on the performance of sales channels
	A.6.2.2	Compensation Planning and Implementation	Develop with a sales channel compensation strategy and oversee the implementation
	A.6.2.3	Sales Training	Develop with provider(s) a sales training program and oversee its successful implementation
	A.6.2.4	Service Fulfillment	Develop with provider(s) a process to ensure fulfillment of services and devices and oversee its successful implementation
	A.6.3	Sales Planning	Together with the provider(s), develop sales plans for all segments of customers
	A.6.3.1	Define the Sales Strategy and Ensure Compliance	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
	A.6.3.2	Sales Forecasting	Develop with provider(s) a short and long term sales forecast and adjust according to changing market trends and dynamics
	A.6.3.2.2	Results Reporting/Trending	Perform to meet expected short and long term sales forecast and adjust according to changing market trends and dynamics.
	A.6.4	Major Accounts Management	Develop major accounts strategy and monitor and produce high level management reports on major accounts performance
	A.6.5	Sales Engineering Support	Provide customized engineering support for major accounts and projects
	A.6.5.1	Facilitate Product Demonstrations	Provide capability to demonstrate products/services to end-users
	A.6.5.2	Support Sales Efforts	Provide customized engineering support for sales efforts on major accounts
	A.6.5.3	Support RFP Development Efforts	Provide customized engineering support for sales proposals and projects
	A.6.5.4	Provide Product Feedback to Engineering	Responsible for providing information on technical and operational issues
	A.7	Product Management	Product management defines, plans, obtains the acceptance for the portfolio of services, applications, and features to meet First Responder requirements.
	A.7.1	Network Services Portfolio Management	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.
	A.7.1.1	Application Developer Ecosystem Product Life Cycle Management	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
	A.7.1.1.1	Application Publishing Management	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.
	A.7.1.1.1.1	Application Upgrading Management	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.
	A.7.1.1.1.2	Application Discovery Management	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.1.1.1.3	Application Purchasing Management	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.
	A.7.1.1.2	Application Review/Rating Systems Management	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.
	A.7.1.1.3	Provide Developer Support	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).
	A.7.1.1.4	Application Fraud Management	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.
	A.7.1.2	Location Services Product Life Cycle Management	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.
	A.7.1.3	IT Services Product Life Cycle Management	Enable general IT service, e.g. not specific to wireless, used by many IT infrastructure components within FirstNet's network domain(s).
	A.7.1.3.1	Domain Name Service (DNS) Management	Enable a Domain Name Service (DNS) that translates domain names to the numerical IP addresses in accordance with all relevant RFCs.
	A.7.1.3.2	Enterprise Security Management	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.
	A.7.1.3.2.1	Digital Certificate Management	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.
	A.7.1.4	Identity Management Product Life Cycle Management	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.
	A.7.1.4.1	Identity Management Auditing & Accounting	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.
	A.7.1.4.2	Federated Identity Management	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.
	A.7.1.4.2.2	Defining & Evolve Trustmarks	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.1.4.3	Define and Support Access Policies	<p>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).</p> <p>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.</p>
	A.7.1.4.4	Manage Authorization Services	<p>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.</p>
	A.7.1.4.5	Manage Authentication Services	<p>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.</p>
	A.7.1.4.5.1	Manage Multi-Factor Authentication	<p>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.</p>
	A.7.1.4.5.2	Manage Single Sign-on	<p>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.</p>
	A.7.1.5	Group Communication (GCSE 3GPP) Product Life Cycle Management	<p>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.</p>
	A.7.1.6	QoS, Priority, and Preemption (QPP) Administration	<p>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.</p>
	A.7.1.6.1	Management and Enablement of Dynamic User Profiles	<p>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.</p>
	A.7.1.6.1.1	Management of Access Class Barring	<p>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.</p>
	A.7.1.6.1.2	Management of QoS Class Identifiers (QCI)	<p>Enable and support of all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.</p>
	A.7.1.6.1.3	Immediate Peril Service Management	<p>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)</p>

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.1.6.1.4	Allocation and Retention Policy (ARP) Management	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.
	A.7.1.6.1.5	Incident Command System (ICS) Service Management	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.
	A.7.1.6.1.5.1	Real Time Priority & Role based QoS Execution	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.
	A.7.1.6.1.6	Processing of Responder Emergency Invocation	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.
	A.7.1.6.1.6.1	Implementation of Immediate Location & Priority	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.
	A.7.1.6.2	Management and Enablement of Static User Profiles	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.
	A.7.1.7	Payment Services Product Life Cycle Management	Manage the product life cycle of the payment feature and capability incorporated in all relevant services and applications provided by the NPSBN
	A.7.1.8	Presence Services Product Life Cycle Management	Presence Services includes the creation of a presence infrastructure. The solution should be compliant with GSM-R 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.
	A.7.1.8.1	Local Status Update Provisioning	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.
	A.7.1.9	Mobile Device Management Product Life Cycle Management	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.
	A.7.2	User Services Portfolio Management	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.
	A.7.2.1	Mission Critical Push-to-talk Voice (3GPP) Product Life Cycle Management	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
	A.7.2.1.1	Security Management for Push to Talk Services	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
	A.7.2.1.2	Group Management/Communications Service Management	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
	A.7.2.2	Broadcast Services Product Life Cycle Management	This function will use a new technology called eMBMS to optimize bandwidth required for broadcast, a type of one to many communications.
	A.7.2.3	Data Services Product Life Cycle Management	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.
	A.7.2.3.1	Video Services Product Management	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.2.3.1.1	Mobile Video Feeds Service Management	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.
	A.7.2.3.1.2	3rd Party Video Service Management	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.
	A.7.2.3.2	CMAS Services Product Management	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.
	A.7.2.3.2.1	Alert Aggregation Service Management	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.
	A.7.2.3.2.2	Alert Dissemination Service Management	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.
	A.7.2.3.2.2.1	Local Delivery Service Management	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.
	A.7.2.3.3	Messaging Product Management	This function includes text messaging, multimedia messaging, and any messaging service needed by PS.
	A.7.2.3.3.1	Email Service Management	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.
	A.7.2.3.3.2	Instant Messaging Service Management	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.
	A.7.2.3.3.3	SMS/MMS Service Management	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
	A.7.2.3.4	M2M Feeds Product Management	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.
	A.7.2.3.4.1	Mission Critical Data Service Management	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.
	A.7.2.3.4.2	Non-Mission Critical Data Service Management	This is a function to transmit routine data, the data that is not crucial to the FirstNet mission as described above.
	A.7.2.3.5	Cloud Services/Hosted Applications Management	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.
	A.7.2.3.5.1	Manage Software as a Service (SaaS)	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.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.2.3.5.2	Manage Big Data Analytics Platform	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.
	A.7.2.3.5.3	Manage Agency Information Homepage	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
	A.7.2.3.5.4	Manage Service Delivery and Installation	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.
	A.7.2.3.5.5	Manage Infrastructure as a Service (IaaS)	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.
	A.7.2.3.5.6	Cloud Service Discovery Management	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.
	A.7.2.4	Direct Mode Product Life Cycle Management	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.
	A.7.2.5	Voice Services Product Life Cycle Management	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.
	A.7.2.5.1	Cellular Telephony Product Management	Voice services available over commercial cellular networks. The NPSBN can enable Voice-over-IP (VoIP) telephony and other open-standard telephony solutions.
	A.7.2.5.1.1	Call Forwarding Service Management	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.
	A.7.2.5.1.2	Voice Mail Service Management	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.
	A.7.2.5.1.3	Ring back tones Service Management	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.
	A.7.2.5.1.4	Supplementary Service Management	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.
	A.7.2.5.1.4.1	Directory Assistance Service Management	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.
	A.7.2.5.1.4.2	Call Waiting Service Management	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.
	A.7.2.5.1.4.3	Caller ID Service Management	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").

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.2.5.2	9-1-1 Services Product Management	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.
	A.7.2.5.2.1	E9-1-1 Service Management	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.
	A.7.2.5.2.1.1	Text To 9-1-1 Service Management	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.
	A.7.2.5.2.2	Provide Connection for NextGen 9-1-1 Service Management	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
	A.7.3	Security Requirements Management	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.
	A.7.5	Product Management Support for FirstNet Industry Efforts	Responsible for supporting industry efforts in product development and management.
	A.7.6	Develop Offers (In Support of Sales)	Responsible for developing special product/service/pricing offers.
	A.7.6.1	Develop Offers for Proposals	Responsible for developing responses to RFPs and other special offers/responses.
	A.7.6.2	Approve Offers for Proposals	Responsible for reviewing and approving special product/service/pricing offers
	A.8	Stakeholder Management and Marketing	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).
	A.8.1	Marketing Strategy	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.
	A.8.1.1	Planning of the Marketing Strategy	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".
	A.8.1.2	Conducting Market Research	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.
	A.8.1.3	Defining Pricing Strategy	Definition of tariff plans to accommodate all public safety needs.
	A.8.1.3.2	Recommendation of Pricing Strategy	FirstNet develops and recommends Pricing Strategy including tariff plans across all services, features and functionality to meet the FirstNet business objectives.
	A.8.1.4	Definition of Near Term Public Safety Product Roadmap	FirstNet led effort to 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.
	A.8.2	Communications Strategy	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.
	A.8.2.2	Branding & Product Positioning Strategy	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.
	A.8.2.3	Media Strategy Support	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.
	A.8.2.4	Social Media Strategy Support	Social Media strategy as used in the advertising or content delivery over social media platforms to First Responders, Agencies, and Secondary users.
	A.8.2.5	Advertising & Promotion Strategy Support	Advertising & Promotion Strategy is the plan to be used for attracting and sustaining the First Responder User base.
	A.8.2.6	Community Relations Support	Support FirstNet in working with local communities to promote public safety communications, including event sponsorships, public awareness drives, etc.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.8.2.7	Event Communications Support	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.)
	A.8.3	Market Analysis	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.
	A.8.3.1	Segmentation Planning	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.
	A.8.3.2	Customer Needs Analysis	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.
	A.8.3.3	User Forecasting & Reporting	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.
	A.8.5	Consultation	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.
	A.8.5.1	State/Federal/Tribal Consultation	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.
	A.8.5.1.1	Support Consultation Efforts	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
	A.8.5.1.4	State/Federal/Tribal Outreach	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
	A.8.5.1.4.2	Events Management Support	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.
	A.8.5.2	State Plan Development	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.
	A.8.5.2.1	Pre State Plan Development Support	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

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.8.5.2.2	Post State Plan Support	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.
	A.8.6	User Fee Administration	Manages user rate plan definitions and associated user fees.
	A.8.6.1	User Fee Determination with Contractor(s)	Provides the venue to come to a mutual agreement on what the reoccurring fees would be to access the network for each user.
	A.8.6.2	User Fee Implementation	Execution of all marketing collateral (e.g. website, flyers, etc.) regarding the user fee structure agreed with FirstNet.
	A.8.7	Definition of Device Portfolio	Responsible for commercial discussions and negotiating with device and embedded application provider(s) to define and build a portfolio of devices.
	A.8.7.1	Commercial Discussions/Negotiations for Devices & Pricing	Commercial discussions and negotiations for FirstNet devices including information gathering, initial proposal and negotiation, and proposal modifications to final contract.
	A.8.7.2	Device Embedded Apps Management	Manage the FirstNet device embedded application requirements working with commercial provider(s) to ensure they are added to the device portfolio.
Blue - Public Safety	A.2.1.2.2	Tier 1 Troubleshooting Agency Support	Agencies will provide the first level of support for users in regards to how to use their devices and applications and new accessories
	A.2.1.3.1.1.2	UICC Installation on Device	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.
	A.2.1.3.1.2	Policy, Apps & Content Management	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.
	A.2.1.3.1.4	Diagnostics Monitoring & Management	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.
	A.2.1.3.1.5	SW, OS & FW Management	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.
	A.2.1.3.1.6	Shared Device Management	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.
	A.2.1.3.1.7	BYOD Management	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.
	A.2.1.3.2	Inventory/Service Fulfillment Management	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.
	A.2.1.3.2.1	Manage Device Returns	The tasks associated with managing the return devices and accessories using online and other systems supported and maintained by the B/operating systems.
	A.2.1.3.2.2	Manage Device Ordering	The tasks associated with managing the ordering of devices and accessories using online and other systems supported and maintained by the B/operating systems.
	A.2.1.3.2.3	Manage Stocking of Devices	The tasks associated with managing the stock of devices and accessories.
	A.2.1.3.2.4	Device and Accessory Inventory Management	The tasks associated with managing the inventory of devices and accessories at agencies.
	A.2.1.3.2.4.1	Installation of In-Vehicle Devices	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.
	A.2.1.3.3	Agency User Subscription Management	Management by the agencies of the individual user activation and deactivation process.
	A.2.1.3.3.1	Local Control User Provisioning & Administration	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.
	A.2.1.3.3.1.1	User Profile Life Cycle Management	Management by the agencies of the individual user profile, services, capabilities, and applications on the device during the user life cycle.
	A.2.1.3.3.1.1.2	Modification of a User Profile	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.
	A.2.1.3.3.1.2	De-Provisioning of Users	Allows an agency to remove a user or device from the NPSBN and delete associated assignments the user had.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description	
Blue - Public Safety	A.2.1.3.3.1.2.1	Rating (Billing) Deactivation	Allows an agency to turn off billing for the individual user or device.	
	A.2.1.3.3.1.2.2	User Profile De-assignment	Allows an agency to turn off the assignment of the user to a profile that remains active (for other users).	
	A.2.1.3.3.1.2.3	Services and Applications Deactivation	Allows an agency to turn off the user or devices assignments to network services and/or device applications.	
	A.2.1.4.1	View Agency Level Network Status	Monitoring network status, such as a local network operations center view for various agencies and/or states.	
	A.2.1.5.3	Training Users on Agency Specific Applications and Procedures	Training users in the usage of agency specific applications and procedures on FirstNet.	
	A.4.10	Implement & Enforce Policy Procedures Across Agencies	Implement and enforce FirstNet security policies, business processes, and operational procedures within the local agencies.	
	A.7.1.4.3.1	PSE Support and Define Local Access Policies	PSEN provides the support and definition of their local access policies for the set up and establishment of PSEN Identity management	
	A.7.2.3.1.3	Video Feeds Service Management	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.	
	Green - FirstNet Only	A.1	FirstNet Program Management and Governance	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.
		A.1.1	FirstNet Executive Guidance	FirstNet Management on the overall execution of the program and FirstNet's strategy
A.1.1.1		Strategic Direction from Board	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.	
A.1.10		Compliance Auditing	Responsible for supporting financial, management and programmatic auditing functions to ensure compliance with all contractual terms and conditions.	
A.1.10.1		Provider(s) Revenue Assurance Auditing and Monitoring	Responsible for auditing and monitoring receivables, collections, and bad debt to ensure compliance with all contractual terms and conditions from provider(s).	
A.1.10.2		Process & Procedure Auditing for Services and Operations	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.	
A.1.10.3		Auditing the Security of Services, Systems, Processes, and Procedures	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.	
A.1.11		Performance Management (QASP)	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.	
A.1.11.1		SLA Compliance Defining & Monitoring	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.	
A.1.11.2		KPI Defining & Monitoring	Responsible for defining and oversight of auditing NPSBN Key Performance Indicators to ensure contract compliance.	
A.1.11.3		Network Monitoring	Monitoring the overall NPSBN network performance. Identifying and resolving performance issues working with the contractors.	
A.1.11.3.1		Network Analytics	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.	
A.1.11.4		Performance Monitoring of System Engineering Lifecycle	Monitoring of the Systems Engineering Lifecycle performance within the contractors' network.	
A.1.12		Change Management	Responsible for discussing and negotiating with provider(s) for changes required on technical, financial or organizational areas based on evolving needs.	
A.1.12.1		Manage Organization Structure	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	
A.1.12.2		Resource Management	Responsible for discussing and negotiation with provider(s) for resource requirement changes in support of change management	
A.1.12.3		Manage Change Work Orders	Responsible for discussing and negotiation with provider(s) for work order changes for the expedient execution of the program and required program changes	
A.1.13		Definition of Network Guidelines	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.	
A.1.13.1		End to End Security Polices	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.	

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.1.13.2	Network Identifiers Policies	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.
	A.1.13.3	Spectrum Management & Usage	The function will create and monitor the Band 14 spectrum management framework with respect to FirstNet, FirstNet provider(s), and opt-out states.
	A.1.13.4	Network Design Objectives	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.
	A.1.14	Roaming Administration	Identify and develop roaming requirements working with the contractors. Oversee the timely implementation of the roaming provider(s)hip agreements.
	A.1.15	Use Case Development	Definition of all possible use cases including M2M for the NPSBN which will drive requirements for product management and network design guidelines
	A.1.15.1	Public Safety Use Case Development	Definition of public safety use cases which will drive product requirements and network design guidelines
	A.1.15.2	Secondary Users via CLA - Use Case Development	Definition of secondary use via CLAs use cases which will drive product requirements and network design guidelines
	A.1.15.3	Others Use Case Development (including M2M)	Definition of other use cases including secondary M2M which will drive product requirements and network design guidelines
	A.1.16	Program Management Oversight	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.
	A.1.16.1	Program/Project Impact Management	Assessment of Program impacts and identifying potential strategies or solutions to mitigate or reduce impacts to a program
	A.1.16.1.1	Schedule Management	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
	A.1.16.1.2	Risk Management	Assessment of Program risks and identifying potential strategies or solutions to mitigate or reduce risks to a program
	A.1.16.1.3	Project Change Management	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
	A.1.16.2	Program/Project Communications	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.
	A.1.16.2.1	Management of Program/Project Status	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.
	A.1.16.2.2	Executive & Board Reporting	Responsible for the creation, delivery and presentation of an Executive Summary Report of all project information, status and completions to the Board
	A.1.17	Sales Management Oversight and Performance Monitoring	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
	A.1.2	Support Industry Relation Communications	Responsible for communications and maintaining good relations with Industries associated with Firstnet including suppliers. Responsible for internal communications of evolving market changes and needs
	A.1.2.1	Conduct Outreach to Public Safety Associations	Responsible for communications and maintaining good relations with various public safety associations
	A.1.2.2	Conduct Outreach to US Industry Associations	Responsible for communications and maintaining good relations with various industry associations
	A.1.2.3	Standards Participation	Responsible for attending and pushing features and capabilities required by public safety in the necessary standards organizations.
	A.1.2.4	International Standards Strategy Development	Responsible for developing an international strategy to collaborate and align with other countries pursuing LTE for public safety in the standards and industry organizations.
	A.1.2.5	Commercial Industry Communications	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.
	A.1.3	Legal Affairs	Responsible for ensuring compliance with the enabling act for FirstNet, and any other laws that may apply to FirstNet
	A.1.3.1	Environmental Compliance Oversight	Function oversees the NPSBN compliance with environmental related laws at all times. For example NEPA.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.1.3.2	Spectrum Management	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.
	A.1.3.3	IAA Administration	Support negotiations on inter-agency agreements that may be required from time to time by FirstNet and monitor the performance of such agreements.
	A.1.3.4	Regulatory Filing Review & Approvals	Review and approve all necessary regulatory filings that is necessary for the rollout of the NPSBN written by the contractors on behalf of FirstNet.
	A.1.3.5	NBPSN Economic Desirability Analysis	Review and approve the economic desirability analysis done by the provider(s) for the rollout of the NPSBN.
	A.1.3.6	Monitor NBPSN Legal & Regulatory Compliance	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.
	A.1.4	Technical Certification Oversight	Oversee the certification process and approved certifications for all equipment, applications and devices to ensure compliance with FirstNet needs and requirements
	A.1.5	Acquisition Management	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
	A.1.5.1	Contract Administration	Responsible for the administration of all contracts which includes packaging and preparation for release, signing, and additions/addendums
	A.1.5.1.1	Contract Life Cycle Management	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
	A.1.5.1.2	Contract Change Management	Responsible for the management of all changes to the contract including, redlines, agreements, addendums, and version control until final contract documents
	A.1.6	Stakeholder Management & Marketing	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.
	A.1.7	Management of Opt-Out States	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
	A.1.7.1	Opt-Out States Monitoring Compliance with Laws, Regulations, Polices	Monitor the network activities in opt-out states to ensure full compliance with the laws, regulations and rules that are applicable to FirstNet
	A.1.7.2	Opt Out State SMLA, Negotiations, and Life Cycle Management	Support SMLA negotiations with opt-out states. Monitor legal compliance on the performance to all SMLAs
	A.1.8	Financial Oversight	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.
	A.1.8.1	Cost Assurance	Provide analysis and reporting of current and future project costs to ascertain the overall sustainability of the program.
	A.1.8.2	FirstNet Revenue Assurance	Responsible for setting up revenue assurance function for auditing and monitoring receivables, collections, and bad debt from all revenue sources
	A.1.8.3	Customer Analytics	Perform analysis of data from customer behavior to help make key business decisions via market segmentation and predictive analytics.
	A.1.9	Oversight of Secondary Use via CLA	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.
	A.2.1.5.1	Training on FirstNet Processes and Procedures	Training provider(s) in FirstNet specific processes and procedures.
	A.2.3	Network Solutions Life Cycle Management	Management and oversight of all engineering activities related to the creation, evolution, and on-going operations of the NPSBN.
	A.2.3.2	System Engineering Life Cycle Oversight	Oversight of the systems engineering architecture, design, and integration of the NPSBN.
	A.2.3.2.1	Concept Development	Concept development of the services and technical functionalities to meet public safety marketing requirements.
	A.2.3.2.2	Requirements Engineering	Product requirements collation to develop engineering guidelines and system requirements.
	A.2.3.2.3	System Architecture Life Cycle Oversight	Oversight of the system architecture for each service provided by the NPSBN.
	A.2.3.2.4	System Design and Development	Systems design and development of the NPSBN within the service development lifecycle.
	A.2.3.2.5	System Integration Oversight	Oversight of systems integration of the NPSBN within the integration activity lifecycle.
	A.2.3.2.6	Test and Evaluation Oversight	Oversight of the testing and evaluation of the NPSBN within the service lifecycle.

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.2.3.2.7	Transition Operation & Maintenance Oversight	Oversight of Transition to Operations and continuing Maintenance for the subject change of the lifecycle integration.
	A.2.3.2.8	System Engineering Life Cycle Assessment	Assessment and optimization of the life cycle process for the NPSBN.
	A.2.3.4	Network Solutions End-to-End Architecture Oversight	The oversight for the development of the overall end-to-end architecture of the NPSBN within each lifecycle integration.
	A.2.3.6	Technical Operations Oversight	Oversight of technical operations and practices within the contractors' network.
	A.2.3.6.1	Oversight of Technology Implementation	Oversight of technology implementation operations and practices of the NPSBN.
	A.2.3.6.2	Technology Risk Management Oversight	Oversight of network risk management operations and practices of the NPSBN.
	A.2.3.6.3	Technology Change Management Oversight	Oversight of network change management operations and practices of the NPSBN.
	A.2.3.6.4	Technology Configuration Management Oversight	Oversight of network configuration management operations and practices of the NPSBN.
	A.2.3.6.5	Technology Refresh Oversight	Oversight of technology evolution planning and implementation of NPSBN.
	A.2.3.6.6	Technical Reviews Gates	Management of all approval gates within the systems engineering lifecycle.
	A.2.3.6.7	Opt-Out State Technical Compliance Oversight	Oversight of opt-out state compliance with FirstNet technical policy, procedure and architecture.
	A.3.4.1.2.2	Feature & Services Roadmap Development	Develop systems features and services roadmap in support of the long term product roadmap
	A.3.4.1.2.2.1	Integration of Long term NSPBN Roadmap	Develop roadmap to integrate long term products into the NPSBN
	A.3.4.1.2.2.2	Standards Roadmap Development for Public Safety	Driving Standards organizations to implement the FirstNet long term roadmap
	A.3.4.2.1	Local Control User Administration Architecture	Provides the local control architecture including user/group profiles and device profiles.
	A.3.4.2.2	Product Development & Engineering	Develop and plan the network and radio products required to provide emergency responders and other public safety users communication services in the NPSBN
	A.3.8.2.4.1.4.2	Conduct PTCRB Certification	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.
	A.3.8.2.5.3.2	Public Safety User Security Monitoring	Monitoring procedures, processes, and timely implementation of functions in security systems to prevent potential security breaches for public safety users.
	A.3.8.2.5.3.3	Federal User Security Monitoring	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.
	A.3.8.2.5.4.1	Public Safety Agency Policy Enforcement	Ensuring public safety agencies to comply with FirstNet's security policies and procedures to prevent potential security breaches.
	A.3.8.2.5.4.2	Federal Security Policy Enforcement	Ensuring federal agencies to comply with FirstNet's security policies and procedures to prevent potential security breaches.
	A.3.8.2.6.6.2	Agency Support for Mitigation Plan Development	Mitigation plans will need to include required support for local, state, or federal agencies. Training exercises must therefore include representation from these constituents.
	A.3.8.3.2	Agency Security Operations Center Management	The contractor(s) will establish protocols working with FirstNet and Agency SOC's to ensure agency applications and data remain secure.
	A.3.8.3.4	NPSBN Security Operations Center Management	Monitoring, detecting, and resolving incidents that may affect the confidentiality, integrity, or availability of network devices, end-user devices, and systems.
	A.3.8.3.4.1	NPSBN Security Intrusion Monitoring & Detection by SOC	Surveillance and identification that an unauthorized access attempt has been made, is occurring, or has occurred.
	A.4.2.2	Monitor Operational Procedure Compliance	Monitor and provide feedback to support the improvement of network operating procedures.
	A.4.3	Define Standard Policies for User Profiles	Develop the user policy profile framework which includes static, dynamic, and subscription profiles.
	A.4.3.1	Static QPP Profile Definition	Develop the user policy profile framework specifically for static, non-emergency situations.
	A.4.3.2	User Subscription Profile Definition	Define all user subscription profiles for NPSBN services such as voice, data, push-to-talk.
	A.4.3.3	Dynamic QPP Profile Definition	Develop the user policy profile framework specifically for dynamic, emergency situations.
	A.4.9	System Engineering Oversight	Oversee systems engineering within NPSBN to ensure compliance of the engineering lifecycle and evolution of the NPSBN.
	A.6.3.2.1	Establishing Sales Targets with Partners and Monitoring Performance	Develop short and long term sales forecast and adjust according to changing market trends and dynamics. Measure target performance achievements
	A.6.3.3	Sales Monitoring and Compliance	Develop with provider(s) and stakeholders a standard sales performance monitoring framework and ensure timely distribution of sales reports

This report shows the functions by FirstNet proposed responsibility.

FirstNet Proposed Functional Owner	Title	Name	Description
	A.7.1.4.2.1	Identify Trustmarks Management	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).
	A.7.1.4.3.2	Support and Define Global Access Policies	FirstNet provides the support and definition of global access policies for the set up and establishment of global Identity management
	A.7.4	Public Safety Product, Feature Roadmap Development	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.
	A.8.1.3.1	Agreement with Provider(s) on Pricing Strategy	FirstNet negotiation and agreement with contractor(s) on pricing strategies for services, features and devices based on FirstNet recommended pricing strategy.
	A.8.2.1	Public Affairs Communications Strategy	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.
	A.8.4	PSAC Engagement	PSAC Engagement involves meeting planning and execution and administrative services of the PSAC, its subcommittees, and working group.
	A.8.5.1.2	Facilitate Resolution of Issues	Coordinating stakeholder input and needs with the provider(s) to come to resolution on user and technical issues.
	A.8.5.1.4.1	Events Management	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.
	A.8.5.2.3	Public Safety Stakeholder Data Collection & Analysis	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.
	A.8.5.2.4	State Plan Change Management	Coordinates stakeholder inputs, requests and engagements relative to changes during the planning, IOC and FOC phase
	A.8.5.2.5	State Plan Delivery to Governor	Consolidate state consultation/outreach data with provider(s) provided support products into a final state plan for signature by the governor.
	A.8.5.3	Governmental Affairs	Interface and consultation with appropriate governmental entities regarding FirstNet.
	A.8.5.3.1	Direct Interaction with Congress	Direct interaction with members of Congress and their staff.
	A.8.5.3.2	Development Federal/Congressional Outreach Plans	Develop and implement the outreach plan for federal and congressional interaction.
	A.8.5.3.3	Communication with Relevant Jurisdiction Committees	Working with the relevant committees of jurisdiction.
	A.8.5.3.4	Communication Development Across Federal Government	Coordinating messaging and message development across the federal government.
	A.8.5.3.5	Develop Hearing Testimonies	Develop hearing testimony and information for congressional hearings and roundtables.
	A.8.5.3.6	Support States on FirstNet Related Items	Direct interaction with state governments including the executive and legislative branches.
	A.8.5.3.8	Support Local Governments on FirstNet related items	Work with city mayors, town councils, and other forms of local government on FirstNet related issues.
	A.8.6.3	User Fee Approval Process Management with NTIA	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.
	A.8.7.3	Device Portfolio Strategy	Define the range of device/accessories types to cover all Public Safety service requirements including pricing.
N/A	A.0	FirstNet	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.