



Operational Architecture Functional Descriptions

Post Special Notice

09/03/15

Table of Contents

- A.0 - FirstNet 16**
- A.1 - FirstNet Program Management and Governance..... 16**
 - A.1.1 - FirstNet Executive Guidance..... 16
 - A.1.1.1 - Strategic Direction from Board..... 16
 - A.1.1.2 - Strategic Planning 16
 - A.1.10 - Compliance Auditing 16
 - A.1.10.1 - Provider(s) Revenue Assurance Auditing and Monitoring 16
 - A.1.10.2 - Process & Procedure Auditing for Services and Operations 16
 - A.1.10.3 - Auditing the Security of Services, Systems, Processes, and Procedures..... 16
 - A.1.11 - Quality Assurance & Performance Managemnt (QASP) 17
 - A.1.11.1 - SLA Compliance Oversight & Evolution 17
 - A.1.11.2 - KPI Compliance & Oversight..... 17
 - A.1.11.3 - Oversight of Prime Contractor's Network Performance Monitoring 17
 - A.1.11.3.1 - Network Performance Analytics Oversight 17
 - A.1.11.4 - Performance Monitoring of System Engineering Lifecycle 17
 - A.1.12 - Change Management 17
 - A.1.12.1 - Oversee & Evolve Organization Structure..... 17
 - A.1.12.2 - Resource Management Oversight..... 17
 - A.1.12.3 - Manage Change Work Orders 17
 - A.1.13 - Oversight & Evolution of Network Guidelines 18
 - A.1.13.1 - End to End Security Policy Oversight..... 18
 - A.1.13.2 - Network Identifiers Policy Oversight..... 18
 - A.1.13.3 - Spectrum Management & Usage Oversight..... 18
 - A.1.13.4 - Network Design Objectives Oversight..... 18
 - A.1.13.4.1 - Oversight of RAN Border Design 18
 - A.1.14 - Roaming Oversight & Approval 18
 - A.1.15 - Use Case Development & Oversight 18
 - A.1.15.1 - Public Safety Use Case Development 18
 - A.1.15.2 - Secondary Users via CLA Use Case Approval..... 19
 - A.1.15.3 - Other Use Case Development (including M2M) 19
 - A.1.16 - Program Management Oversight..... 19
 - A.1.16.1 - Program/Project Impact Management 19
 - A.1.16.1.1 - Schedule Management Oversight 19
 - A.1.16.1.2 - Risk Management Oversight 19
 - A.1.16.1.3 - Project Change Management..... 19
 - A.1.16.2 - Program/Project Communications Oversight 19
 - A.1.16.2.1 - Management of Program/Project Status Oversight..... 19
 - A.1.16.2.2 - Executive & Board Reporting 20
 - A.1.17 - Sales Management Oversight and Performance Monitoring..... 20
 - A.1.18 - Customer Care Oversight & Performance Monitoring..... 20
 - A.1.2 - Industry Relation Communications Oversight..... 20
 - A.1.2.1 - Conduct Outreach to Public Safety Associations..... 20
 - A.1.2.2 - Conduct Outreach to US Industry Associations..... 20
 - A.1.2.5 - Commercial Industry Communications 20
 - A.1.3 - Legal Affairs Oversight..... 20

A.1.3.1 - Environmental Compliance Oversight.....	20
A.1.3.2 - Spectrum Management Oversight.....	20
A.1.3.3 - IAA Administration.....	20
A.1.3.4 - Regulatory Filing Review & Approvals.....	21
A.1.3.5 - NPSBN Economic Desirability Analysis Approval.....	21
A.1.3.6 - Monitor NPSBN Legal & Regulatory Compliance.....	21
A.1.4 - Technical Certification Oversight.....	21
A.1.5 - Acquisition Management Oversight.....	21
A.1.5.1 - Contract Administration.....	21
A.1.5.1.1 - Contract Life Cycle Oversight & Management.....	21
A.1.5.1.2 - Contract Change Management.....	21
A.1.6 - Stakeholder Oversight of Marketing & Communications.....	21
A.1.7 - Opt Out States Oversight & Engagement.....	21
A.1.7.1 - Opt Out States Monitoring Compliance with Laws, Regulations, Policies.....	22
A.1.7.2 - Opt Out State SMLA, Negotiations, and Life Cycle Management.....	22
A.1.8 - Financial Oversight.....	22
A.1.8.1 - Cost Assurance.....	22
A.1.8.2 - FirstNet Revenue Assurance.....	22
A.1.8.3 - Customer Analytics Oversight.....	22
A.1.9 - Oversight of Secondary Use via CLA.....	22
A.2 - Life Cycle Management.....	22
A.2.1 - User Management.....	22
A.2.1.1 - User Security Administration.....	22
A.2.1.1.1 - User Fraud Management.....	23
A.2.1.2 - Customer Service Process Development.....	23
A.2.1.2.1 - Customer Service For Tier 2+ Support.....	23
A.2.1.2.2 - Tier 1 Troubleshooting Agency Support.....	23
A.2.1.2.3 - Provide Tier 1 type Troubleshooting Public Safety Entity support.....	23
A.2.1.3 - Public Safety Entity Management.....	23
A.2.1.3.1 - Device Administration.....	23
A.2.1.3.1.1 - UE (User Equipment) Management.....	23
A.2.1.3.1.1.1 - Nationwide IMEI/UICC Inventory Management.....	23
A.2.1.3.1.1.2 - UICC Installation on Device.....	24
A.2.1.3.1.1.3 - Manage, Stock, & Distribution of Hardware.....	24
A.2.1.3.1.2 - Policy, Apps & Content Administration.....	24
A.2.1.3.1.3 - Over The Air (OTA) Management.....	24
A.2.1.3.1.4 - Diagnostics Monitoring and Administration.....	24
A.2.1.3.1.5 - SW, OS & FW Management and Administration.....	24
A.2.1.3.1.5.1 - SW, OS & FW Management.....	24
A.2.1.3.1.5.2 - SW, OS & FW Administration.....	24
A.2.1.3.1.6 - Shared Device Management.....	25
A.2.1.3.1.7 - BYOD Administration.....	25
A.2.1.3.2 - Inventory/Service Fulfillment Management.....	25
A.2.1.3.2.1 - Manage Device Returns.....	25
A.2.1.3.2.2 - Manage Device Ordering.....	25
A.2.1.3.2.3 - Manage Stocking of Devices.....	25
A.2.1.3.2.4 - Device and Accessory Inventory Management.....	25

A.2.1.3.2.4.1 - Installation of In Vehicle Devices.....	25
A.2.1.3.3 - Agency User Subscription Management	25
A.2.1.3.3.1 - Local Control User Provisioning & Administration	25
A.2.1.3.3.1.1 - User Profile Life Cycle Management	25
A.2.1.3.3.1.1.2 - Modification of a User Profile	26
A.2.1.3.3.1.2 - De Provisioning of Users.....	26
A.2.1.3.3.1.2.1 - Rating (Billing) Deactivation	26
A.2.1.3.3.1.2.2 - User Profile De assignment	26
A.2.1.3.3.1.2.3 - Services and Applications Deactivation.....	26
A.2.1.3.3.1.2.3.1 - Communications Groups Deactivation.....	26
A.2.1.3.3.1.3 - User Administration: Provisioning of Users, User Profile Assignment, Rating (Billing) Activation.....	26
A.2.1.3.3.1.3.1 - User Profile Assignment	26
A.2.1.3.3.1.3.2 - Rating (Billing) Activation	26
A.2.1.3.3.1.3.3 - Installation of Services & Applications	26
A.2.1.3.3.1.3.3.1 - Communications Groups Implementation.....	26
A.2.1.4 - Agency/State Network Monitoring	26
A.2.1.4.1 - View Agency Level Network Status	27
A.2.1.4.2 - Critical Outage Notification to Dispatch Center.....	27
A.2.1.5 - End User Training	27
A.2.1.5.1 - Training on FirstNet Processes and Procedures.....	27
A.2.1.5.2 - Training on FirstNet Hosted Apps and Network Services	27
A.2.1.5.3 - Training Users on Agency Specific Applications and Procedures.....	27
A.2.1.6 - Manage Individually Liable Accounts	27
A.2.1.6.1 - Provide Verification Services and User Provisioning.....	27
A.2.1.6.2 - Support User Purchasing	27
A.2.1.6.2.1 - Develop Process for User Purchasing.....	27
A.2.1.6.2.2 - Approve Process for User Purchasing	27
A.2.1.6.3 - Provide Tier 1 Support.....	27
A.2.1.7 - Service Quality Evaluation from PS User Perspective and Improvement Activities.....	27
A.2.2 - Supply Chain Management	28
A.2.3 - Network Solutions Life Cycle Management	28
A.2.3.1 - Technical Project Management.....	28
A.2.3.1.1 - Technical Schedule & Risk Management	28
A.2.3.1.2 - Engineering & Integration Risk Management	28
A.2.3.2 - System Engineering Life Cycle Oversight.....	28
A.2.3.2.1 - Concept Development.....	28
A.2.3.2.2 - Requirements Engineering	28
A.2.3.2.3 - System Architecture Life Cycle Oversight.....	28
A.2.3.2.4 - System Design and Development.....	28
A.2.3.2.5 - System Integration Oversight.....	28
A.2.3.2.6 - Test and Evaluation Oversight.....	28
A.2.3.2.7 - Transition Operation & Maintenance Oversight.....	29
A.2.3.2.8 - System Engineering Life Cycle Assessment	29
A.2.3.3 - Technical Strategy	29
A.2.3.3.1 - Develop Technical Strategy	29
A.2.3.3.2 - Approve Technical Strategy.....	29

A.2.3.4 - Network Solutions End to End Architecture Oversight	29
A.2.3.5 - Supply Chain Management Oversight	29
A.2.3.6 - Technical Operations Oversight	29
A.2.3.6.1 - Oversight of Technology Implementation.....	29
A.2.3.6.2 - Technology Risk Management Oversight.....	29
A.2.3.6.3 - Technology Change Management Oversight	29
A.2.3.6.4 - Technology Configuration Management Oversight	29
A.2.3.6.5 - Technology Refresh Oversight.....	29
A.2.3.6.6 - Technical Review Gates	29
A.2.3.6.7 - Opt Out State Technical Compliance Oversight	30
A.3 - Engineering & Network Operations.....	30
A.3.1 - Network Financial Administration.....	30
A.3.1.1 - Network CAPEX/OPEX Forecasting.....	30
A.3.1.2 - Network Financial Control.....	30
A.3.1.3 - Business Case Development/Analysis	30
A.3.1.4 - Actual Network Spend Reporting.....	30
A.3.2 - Network Deployment	30
A.3.2.1 - Installation of Network Elements.....	30
A.3.2.2 - Transmission Network Installation.....	30
A.3.2.3 - Site Acquisition Secure & Preparation	31
A.3.2.4 - Warehousing/Inventory (Fixed Asset Management)	31
A.3.2.5 - Transmission Systems Ordering	31
A.3.3 - Priority & QoS Administration.....	31
A.3.3.1 - Profile Configuration Setup	31
A.3.3.2 - Implement Profile Changes	31
A.3.3.3 - Drive Supplier Roadmap for QPP.....	31
A.3.4 - Engineering & Planning	31
A.3.4.1 - Long Term Feature, Function, and Technology Planning.....	31
A.3.4.1.1 - Proof of Concept & Field Testing.....	32
A.3.4.1.1.1 - Approve Test and Trial Recommendation.....	32
A.3.4.1.1.2 - Perform Research, Test, and Trial of New Technology, Service, and Features.....	32
A.3.4.1.1.3 - Prototype Device Testing	32
A.3.4.1.1.4 - Prototype RAN Feature Testing.....	32
A.3.4.1.1.5 - Prototype Services Testing	32
A.3.4.1.1.6 - Participation & Approval of Proof of Concept & Field Testing.....	32
A.3.4.1.2 - Long Term Product Management	32
A.3.4.1.2.1 - Customer Feedback for Long Term Services	32
A.3.4.1.2.1.1 - Sales Feedback for Long Term Services.....	33
A.3.4.1.2.1.2 - Outreach Feedback for Long Term Services.....	33
A.3.4.1.2.2 - Feature & Services Roadmap Development.....	33
A.3.4.1.2.2.1 - Integrate Features & Services into Long term NPSBN Roadmap	33
A.3.4.1.2.2.2 - Standards Roadmap Development for Public Safety	33
A.3.4.1.3 - Long Term Feature Feasibility Analysis	33
A.3.4.1.4 - Supplier Roadmap Coordination	33
A.3.4.1.5 - Global and US Standards Participation, Alignment and Collaboration	33
A.3.4.1.5.1 - Global and US Standards Strategy – Approval of final strategy and tactics.....	33

A.3.4.1.5.2 - Global and US Standards Strategy, Develop Strategy and propose to FirstNet	33
A.3.4.1.5.3 - Global and US Standards Participation – FirstNet, Prime Vendor, and FirstNet/Vendor’s Ecosystem Partners.....	34
A.3.4.1.5.3.1 - FirstNet Participation	34
A.3.4.1.5.3.2 - Prime Contractor and FirstNet EcoSystem Participation	34
A.3.4.2 - Network Design & Architecture	34
A.3.4.2.2 - Product Development & Engineering.....	34
A.3.4.2.2.1 - Mission Critical PTT Engineering & Design	34
A.3.4.2.2.2 - Group Communications Engineering & Design	34
A.3.4.2.2.4 - Location Platform Engineering & Design.....	34
A.3.4.2.2.5 - IMS Platform Engineering & Design	34
A.3.4.2.2.5.1 - VoLTE Engineering & Design	34
A.3.4.2.2.5.2 - Other IMS Services Engineering & Design.....	34
A.3.4.2.2.5.3 - Presence Engineering & Design.....	35
A.3.4.2.2.5.4 - IP Messaging Engineering & Design	35
A.3.4.2.2.6 - Broadcast Platform Engineering & Design	35
A.3.4.2.2.7 - Mobile Device Management Systems Engineering & Design.....	35
A.3.4.2.2.7.1 - Multi-Tenant Management Engineering & Design.....	35
A.3.4.2.2.7.10 - Mobility Management Systems Engineering & Design	35
A.3.4.2.2.7.2 - Policy & Content Management Engineering & Design.....	35
A.3.4.2.2.7.3 - Over The Air (OTA) Updates Engineering & Design.....	35
A.3.4.2.2.7.4 - Mobile Diagnostics, Polling, & Reporting Tools Engineering & Design	35
A.3.4.2.2.7.5 - Software, OS, & Firmware Management Tools and Processes Engineering & Design.....	36
A.3.4.2.2.7.6 - Tethered Device Updates Engineering & Design.....	36
A.3.4.2.2.7.7 - Configuration Management Tools and Systems Engineering & Design	36
A.3.4.2.2.7.8 - BYOD Tools and Methods Enablement Engineering & Design.....	36
A.3.4.2.2.7.9 - UICC/SIM Management Engineering & Design	36
A.3.4.2.2.8 - Direct Mode Communications Engineering & Design	36
A.3.4.2.2.8.1 - Direct Mode Communications Engineering	36
A.3.4.2.2.8.2 - Discovery Systems Engineering	36
A.3.4.2.3 - Transmission Systems Management	36
A.3.4.2.3.2 - Transmission Systems Forecasting	37
A.3.4.2.3.3 - Transmission Systems Design.....	37
A.3.4.2.4 - Core Network Architecture & Design	37
A.3.4.2.4.1 - Core Architecture Design	37
A.3.4.2.4.2 - Capacity Planning	37
A.3.4.2.4.3 - Core Software License Management	37
A.3.4.2.5 - Traffic Management	37
A.3.4.2.5.1 - Traffic Monitoring & Reporting.....	37
A.3.4.2.5.2 - Traffic Forecasting	37
A.3.4.2.6 - Radio Network Planning & Design.....	38
A.3.4.2.6.1 - RAN License Management	38
A.3.4.2.6.2 - RAN Coverage Engineering.....	38
A.3.4.2.6.3 - Deployables Engineering	38
A.3.4.2.6.4 - RAN Capacity Engineering	38

A.3.4.2.6.5 - RAN Integration of Rural Carriers, Other Provider(s) networks, Opt out States for Boundary Areas	38
A.3.4.2.7 - Application Platform Design	38
A.3.4.2.7.1 - Mobile Application Development Platform Design.....	39
A.3.4.2.7.1.1 - Developer Portal Design.....	39
A.3.4.2.7.1.2 - Mobile Application Framework Design	39
A.3.4.2.7.1.3 - Develop SDKs and Development Tools	39
A.3.4.2.7.1.4 - Develop Application Test Platform.....	39
A.3.4.2.7.2 - Design App Store	39
A.3.4.2.7.3 - Design Service Delivery Platform Development.....	39
A.3.4.2.7.3.1 - South Facing API Implementation	40
A.3.4.2.7.3.2 - North Facing API Implementation	40
A.3.4.2.8 - System Hardening Design.....	40
A.3.4.2.8.1 - Reliability Design	40
A.3.4.2.8.2 - Resiliency Design	40
A.3.4.2.8.3 - Disaster Recovery Planning/Design.....	40
A.3.4.2.9 - Cloud Services Administration.....	40
A.3.4.2.9.1 - Develop and Manage Agency Information Homepage	41
A.3.4.2.9.2 - Develop and Manage Application Hosting	41
A.3.4.2.9.3 - Develop and Manage Cloud Services	41
A.3.4.2.9.4 - Develop BigData Analytic Platform and Associated Services	41
A.3.4.3 - End to End NPSBN Architecture Definition	41
A.3.5 - Business Support Systems (BSS) Management	41
A.3.5.1 - Local Control: Service & User Provisioning	42
A.3.5.2 - Billing Administration	42
A.3.5.2.1 - Billing Reporting	42
A.3.5.2.1.1 - Usage Reporting	42
A.3.5.2.1.2 - Billing Data Analytics	42
A.3.5.2.2 - Revenue Assurance (Fraud Management).....	42
A.3.5.2.3 - Roaming Billing Administration	42
A.3.5.2.4 - Opt Out State Billing Administration	42
A.3.5.2.5 - Secondary Usage via CLA Billing Administration	43
A.3.5.2.6 - Invoicing & Billing	43
A.3.5.2.7 - Rating & Pricing Develop/Implement platforms and Systems	43
A.3.5.3 - Business Intelligence Develop/Implement platforms and Systems	43
A.3.5.3.1 - User Business Intelligence Data Analytics	43
A.3.5.4 - Billing Systems Maintenance.....	43
A.3.5.4.1 - Billing Profiles Develop and Implement	43
A.3.5.4.2 - Mediation Platform Administration	43
A.3.5.4.3 - Billing Software Updates	44
A.3.5.4.4 - Billing System Reporting.....	44
A.3.5.4.4.1 - Billing Intelligence Data Analytics.....	44
A.3.5.4.4.2 - System Usage Reporting.....	44
A.3.5.5 - Customer Relationship Management (CRM).....	44
A.3.5.6 - Data Storage Administration	44
A.3.6 - Performance Management	44
A.3.6.1 - Service Optimization	44
A.3.6.2 - Parameter Standardization	44

A.3.6.3 - Network Optimization	45
A.3.6.3.1 - Outage Mitigation	45
A.3.6.3.2 - Coverage Tuning.....	45
A.3.6.3.3 - Capacity Tuning	45
A.3.6.3.4 - Configuration Optimization.....	45
A.3.6.3.5 - Coverage Field Testing & Measurement	45
A.3.6.4 - KPI Monitoring.....	45
A.3.7 - O&M Interfaces & Tools	45
A.3.7.1 - Data Storage for Tools Administration.....	45
A.3.7.2 - Field Measurement Tool Management.....	45
A.3.7.3 - Element Management System Administration	46
A.3.7.4 - KPI Development and Implementation	46
A.3.7.5 - KPI Reporting	46
A.3.7.5.1 - Network Events & Alerting Administration.....	46
A.3.8 - Network Management	46
A.3.8.2 - Operations & Maintenance	46
A.3.8.2.1 - Experience Center & Training Creation and Management	46
A.3.8.2.1.1 - Public Safety ICS Training including Lab Training	46
A.3.8.2.1.2 - NPSBN feature demonstrations in Lab.....	46
A.3.8.2.1.3 - Lab Implementation & Updates Management	47
A.3.8.2.2 - Network Maintenance.....	47
A.3.8.2.2.1 - Hardware & Software Updates	47
A.3.8.2.2.2 - Equipment or Service Repair.....	47
A.3.8.2.2.3 - Equipment Spares Management.....	47
A.3.8.2.2.4 - Preventative Maintenance	47
A.3.8.2.3 - Manage Network Operations	47
A.3.8.2.3.1 - Manage Network, Roaming, and Identifier Configuration.....	47
A.3.8.2.3.1.1 - Roaming Configuration Management.....	47
A.3.8.2.3.1.2 - Network Identifier Management	48
A.3.8.2.3.1.3 - Managing Network Settings For Mobile Devices	48
A.3.8.2.3.2 - Lawful Intercept Management (CALEA) Implementation	48
A.3.8.2.3.2.1 - Other Services Intercept Authorization & Execution (e.g. location)	48
A.3.8.2.3.2.2 - Cyber Monitoring Authorization & Execution.....	48
A.3.8.2.3.2.3 - Signaling Intercept Authorization & Execution	48
A.3.8.2.3.2.4 - Voice Intercept Authorization & Execution.....	48
A.3.8.2.3.2.5 - Data Intercept Authorization & Execution	48
A.3.8.2.3.2.6 - Messaging Intercept (SMS/MMS) Authorization & Execution.....	48
A.3.8.2.3.3 - Management Network Element, Software, and Feature Releases	49
A.3.8.2.3.3.1 - New or Upgrade Network Elements Release Management	49
A.3.8.2.3.3.2 - New or Upgrade Software Release Management.....	49
A.3.8.2.3.3.3 - New or Upgrade Feature or Functionality Release Management.....	49
A.3.8.2.3.4 - Device Management Systems Operations	49
A.3.8.2.3.4.1 - Operating the Multi Tenant Management Access and Permissions	49
A.3.8.2.3.4.10 - Perform Device Mobility Management.....	49
A.3.8.2.3.4.2 - Operating Device Policies & Content Management.....	49
A.3.8.2.3.4.3 - Management of device configuration and updates	49
A.3.8.2.3.4.4 - Managing Tools for Diagnostics, Polling, & Reporting on the Device	50
A.3.8.2.3.4.5 - Mobile Device Software, OS, & Firmware Management	50

A.3.8.2.3.4.6 - Updating Mobile Device Via Tethering Arrangements.....	50
A.3.8.2.3.4.7 - Operating and Maintaining Mobile Device Configuration Management.....	50
A.3.8.2.3.4.8 - Updating and Tracking Mobile Devices for BYOD Users	50
A.3.8.2.3.4.9 - Providing UICC/SIM Management for Devices.....	50
A.3.8.2.3.5 - Network Impairment Support and Reporting	50
A.3.8.2.3.5.1 - After Action Reporting	50
A.3.8.2.3.5.2 - Provide technical support for issue resolution	51
A.3.8.2.3.5.3 - Tier 2 Support.....	51
A.3.8.2.3.5.4 - Tier 3 Support.....	51
A.3.8.2.3.6 - Problem Management.....	51
A.3.8.2.3.6.1 - Problem Investigation & Resolution.....	51
A.3.8.2.3.6.2 - Continual Service Improvement.....	51
A.3.8.2.3.7 - Administer Local Control System	51
A.3.8.2.3.7.1 - Administer and Maintain Local Control User Service.....	51
A.3.8.2.3.7.1.1 - Develop guidelines for Static and Dynamic Profiles.....	51
A.3.8.2.3.7.1.2 - Develop Guidelines for NIMS ICS	52
A.3.8.2.3.7.2 - Develop Local Control User Operations Guidelines	52
A.3.8.2.4 - Perform Quality Assurance, Testing, and Certification	52
A.3.8.2.4.1 - Design, execution, and acceptance of user equipment carrier tests	52
A.3.8.2.4.1.3 - Device Performance Testing.....	52
A.3.8.2.4.1.3.2 - Device Interoperability Testing	52
A.3.8.2.4.1.3.5 - Application Interoperability Testing.....	52
A.3.8.2.4.1.4 - Manage User Equipment FCC and PTCRB Certification.....	52
A.3.8.2.4.1.4.1 - Conduct FCC Type Certification.....	52
A.3.8.2.4.1.4.2 - Conduct PTCRB Certification	52
A.3.8.2.4.1.5 - Device Administration of Secondary User via CLA	52
A.3.8.2.4.2 - Field Test Execution.....	53
A.3.8.2.4.2.1 - Major Software/Hardware Upgrade Testing.....	53
A.3.8.2.4.2.2 - New Services Testing.....	53
A.3.8.2.4.3 - Execution of Interconnection Testing	53
A.3.8.2.4.3.1 - Execution of Opt out RAN Interconnection testing.....	53
A.3.8.2.4.3.2 - Execution of ISP/PSTN Interconnection Testing.....	53
A.3.8.2.4.3.3 - Execution of Roaming Interconnection Testing	53
A.3.8.2.4.3.4 - Execution of Inter carriers Interconnection Testing.....	53
A.3.8.2.4.3.4.1 - WiFi Interconnection Testing	53
A.3.8.2.4.3.5 - Execution of Backhaul & Backbone Interconnection Testing.....	54
A.3.8.2.4.3.6 - Execution of PSEN Interconnection Testing	54
A.3.8.2.4.3.7 - Execution of Cloud Services Interconnection Testing	54
A.3.8.2.4.4 - Perform Application Certification.....	54
A.3.8.2.4.4.1 - Perform 3rd Party Sandbox Certification	54
A.3.8.2.4.4.2 - Perform FirstNet Hosted Application Certification	54
A.3.8.2.4.5 - Perform NPSBN System Integration Testing	54
A.3.8.2.4.5.1 - Device Manager Platform Testing	54
A.3.8.2.4.5.2 - RAN Equipment Testing.....	54
A.3.8.2.4.5.3 - Core Network Equipment Testing	55
A.3.8.2.4.5.4 - Application Delivery Platform Testing.....	55
A.3.8.2.4.6 - Manage Service Experience.....	55
A.3.8.2.4.6.1 - Perform Service Experience Data Analytics	55

A.3.8.2.4.6.2 - Manage Service Availability.....	55
A.3.8.2.4.6.3 - Manage Service Capacity.....	55
A.3.8.2.4.6.4 - Manage Service Level.....	55
A.3.8.2.5 - Security Systems Management.....	55
A.3.8.2.5.1 - Physical Security Management.....	56
A.3.8.2.5.2 - Personnel Identity Management.....	56
A.3.8.2.5.3 - Cyber Security Monitoring.....	56
A.3.8.2.5.3.1 - Security Threat Mitigation.....	56
A.3.8.2.5.3.2 - Public Safety User Security Monitoring.....	56
A.3.8.2.5.3.3 - Federal User Security Monitoring.....	56
A.3.8.2.5.4 - Security Policy Enforcement.....	56
A.3.8.2.5.4.1 - Public Safety Agency Policy Enforcement.....	56
A.3.8.2.5.4.2 - Federal Security Policy Enforcement.....	56
A.3.8.2.6 - Disaster Response & Recovery (NIMS Types 1,2,3) & Major Planned Event Operations.....	57
A.3.8.2.6.1 - Network Restoration.....	57
A.3.8.2.6.2 - Disaster response information gathering.....	57
A.3.8.2.6.3 - Agency Coordination.....	57
A.3.8.2.6.4 - Event Tracking.....	57
A.3.8.2.6.5 - Event Preparation.....	57
A.3.8.2.6.5.1 - Incident Setup & Management.....	57
A.3.8.2.6.6 - NPSBN Mitigation Plan Development.....	57
A.3.8.2.6.6.1 - NPSBN Mitigation Implementation.....	58
A.3.8.2.6.6.2 - Agency Support for NPSBN Mitigation Plan Development.....	58
A.3.8.2.6.7 - Post Incident & Event Analysis Reporting.....	58
A.3.8.3 - Perform Network Monitoring.....	58
A.3.8.3.1 - Manage Network Operations Center.....	58
A.3.8.3.1.1 - Manage Trouble Ticket Process.....	58
A.3.8.3.1.2 - Manage Network Issues.....	58
A.3.8.3.2 - Manage Agency Security Operations Center.....	58
A.3.8.3.2.1 - Manage Intrusion Protection System.....	58
A.3.8.3.2.2 - Perform Intrusion Recovery Procedures.....	59
A.3.8.3.2.3 - Internal Security Compromise Detection.....	59
A.3.8.3.2.4 - External Security Intrusion Detection.....	59
A.3.8.3.3 - Manage Federal Security Operations Center.....	59
A.3.8.3.4 - Manage NPSBN Security Operations Center.....	59
A.3.8.3.4.1 - Perform NPSBN Security Intrusion Monitoring & Detection by SOC.....	59
A.3.8.3.4.2 - Perform Device Malware Detection and Deletion.....	59
A.3.9 - Field Testing for Public Safety Services.....	59
A.3.9.1 - Public Safety Use Case Testing and Verification.....	59
A.3.9.2 - Public Safety User Experience Assurance & Verification.....	59
A.3.9.3 - Public Safety Service Quality and Capability Assurance.....	60
A.4 - Policies & Procedures.....	60
A.4.1 - Define, Implement, and Monitor Provisioning Policies & Procedures.....	60
A.4.1.1 - Define and Implement Provisioning Procedures.....	60
A.4.1.2 - Monitor Provisioning Policy & Procedure Compliance.....	60
A.4.10 - Implement and Enforce Policy Procedures Across Local Public Safety Entities.....	60

A.4.2 - Define, Implement, and Monitor Network Policies & Procedures.....	60
A.4.2.1 - Define and Implement Operational Procedures	60
A.4.2.2 - Monitor Operational Procedure Compliance.....	60
A.4.3 - Define Standard Definitions for Static QPP, Dynamic QPP, and User Subscription profiles	61
A.4.3.1 - Static QPP Profile Definition.....	61
A.4.3.2 - User Subscription Profile Definition	61
A.4.3.3 - Dynamic QPP Profile Definition.....	61
A.4.4 - Define, Implement, and Monitor Billing Policies & Procedures.....	61
A.4.5 - Security and Network Operations Best Practices.....	61
A.4.5.1 - Develop Security and Network Operations Best Practices.....	61
A.4.5.2 - Approve Security and Network Operations Best Practices	61
A.4.6 - Develop Customer Care Policies & Procedures.....	61
A.4.7 - Develop Marketing Policies & Procedures	61
A.4.8 - Develop Sales Policies & Procedures.....	62
A.4.9 - System Engineering Oversight of Policies & Procedures.....	62
A.5 - NPSBN Services Program Management & Contract Compliance.....	62
A.5.1 - Agency Administration Program Support.....	62
A.5.2 - Services Program Support & Reporting.....	62
A.5.3 - Network Operation Program Support.....	62
A.5.4 - Contract Financial Administration.....	62
A.5.4.1 - Revenue Variance Reporting.....	62
A.5.4.2 - Cost Variance Reporting	62
A.5.4.2.1 - Cost of Sales Reporting.....	63
A.5.4.2.2 - General & Administrative Cost Reporting	63
A.5.4.3 - Contract Performance Tracking.....	63
A.5.5 - Regulatory Management.....	63
A.5.5.1 - Preparation of Regulatory Filings and Forms	63
A.5.5.2 - NPSBN Regulatory Compliance Monitoring & Reporting.....	63
A.5.5.3 - Reporting of Opt Out State Compliance.....	63
A.5.6 - Legal Support.....	63
A.5.6.1 - Legal Compliance Monitoring & Reporting	63
A.6 - Sales Management	64
A.6.1 - Public Safety Entity Sales Channel Management	64
A.6.1.1 - Public Safety Sales	64
A.6.1.1.1 - Law Enforcement Sales.....	64
A.6.1.1.2 - Fire Department Sales	64
A.6.1.1.3 - EMS Sales.....	64
A.6.1.1.4 - 911 Sales.....	64
A.6.1.1.5 - Others Entity Sales.....	64
A.6.1.2 - Federal Sales.....	64
A.6.1.2.1 - Federal Public Safety Sales	64
A.6.1.2.2 - Federal Non Public Safety Sales	64
A.6.1.3 - State Government and Tribal Sales.....	65
A.6.1.3.1 - State Government and Tribal Public Safety Sales	65
A.6.1.3.2 - State Government and Tribal Non Public Safety Sales.....	65

A.6.1.4 - Retail Sales.....	65
A.6.1.4.1 - Retail/Provider(s) Sales	65
A.6.1.4.2 - Retail/3rd Party Sales	65
A.6.1.5 - Internet and Telemarketing Sales	65
A.6.1.6 - Utility Responder Sales.....	65
A.6.1.6.1 - Sales to Utilities	65
A.6.1.7 - Account Management.....	65
A.6.1.7.1 - Customer Acquisition Planning & Implementation.....	65
A.6.1.7.2 - Customer Retention/Winback Planning and Implementation.....	66
A.6.1.7.3 - Account Planning.....	66
A.6.1.7.3.1 - Conduct Account Planning	66
A.6.1.7.3.2 - Account Planning Compliance.....	66
A.6.1.7.4 - Special Pricing Development.....	66
A.6.1.8 - User Migration and Evolution	66
A.6.2 - Sales Operations & Support	66
A.6.2.1 - Sales Reporting.....	66
A.6.2.2 - Compensation Planning and Implementation.....	66
A.6.2.3 - Sales Training.....	66
A.6.2.4 - Service Fulfilment.....	66
A.6.3 - Sales Planning.....	66
A.6.3.1 - Sales Strategy and Compliance.....	67
A.6.3.1.1 - Identify priority elements of Sales Strategy	67
A.6.3.1.2 - Develop Sales Strategy	67
A.6.3.1.3 - Approve Sales Strategy.....	67
A.6.3.2 - Sales Forecasting	67
A.6.3.2.1 - Sales Targets and Monitoring Performance.....	67
A.6.3.2.2 - Sales Results Reporting/Trends.....	67
A.6.3.3 - Sales Monitoring and Compliance.....	67
A.6.4 - Major Accounts Management.....	67
A.6.5 - Sales Engineering Support.....	67
A.6.5.1 - Facilitate Product Demonstrations.....	67
A.6.5.2 - Support Sales Efforts	67
A.6.5.3 - Support RFP Development Efforts.....	68
A.6.5.4 - Provide Product Feedback to Engineering	68
A.7 - Product Management.....	68
A.7.1 - Network Services Portfolio Management	68
A.7.1.1 - Application Developer Ecosystem Product Life Cycle Management	68
A.7.1.1.1 - Application Publishing Management	68
A.7.1.1.1.1 - Application Upgrading Management	68
A.7.1.1.1.2 - Application Discovery Management	68
A.7.1.1.1.3 - Application Purchasing Management	68
A.7.1.1.2 - Application Review/Rating Systems Management	69
A.7.1.1.3 - Provide Developer Support	69
A.7.1.1.4 - Application Fraud Management.....	69
A.7.1.2 - Location Services Product Life Cycle Management.....	69
A.7.1.3 - IT Services Product Life Cycle Management.....	69
A.7.1.3.1 - Domain Name Service (DNS) Management	69

A.7.1.3.2 - Enterprise Security Management.....	69
A.7.1.3.2.1 - Digital Certificate Management	69
A.7.1.4 - Identity Management Product Life Cycle Management	70
A.7.1.4.1 - Identity Management Auditing & Accounting	70
A.7.1.4.2 - Federated Identity Management	70
A.7.1.4.2.1 - Identity Trustmarks Management.....	70
A.7.1.4.2.2 - Defining & Evolve Trustmarks	70
A.7.1.4.2.2.1 - Defining Trustmarks	70
A.7.1.4.2.2.2 - Approve Trustmarks	71
A.7.1.4.3 - Define and Support Access Policies.....	71
A.7.1.4.3.1 - PSE Support and Define Local Access Policies.....	71
A.7.1.4.3.2 - Support and Define Global Access Policies	71
A.7.1.4.4 - Manage Authorization Services.....	71
A.7.1.4.5 - Manage Authentication Services.....	71
A.7.1.4.5.1 - Manage Multi Factor Authentication	72
A.7.1.4.5.2 - Manage Single Sign on.....	72
A.7.1.5 - Group Communication (GCSE 3GPP) Product Life Cycle Management	72
A.7.1.6 - QoS, Priority, and Preemption (QPP) Administration	72
A.7.1.6.1 - Management and Enablement of Dynamic User Profiles	72
A.7.1.6.1.1 - Management of Access Class Barring.....	72
A.7.1.6.1.2 - Management of QoS Class Identifiers (QCI)	73
A.7.1.6.1.3 - Immediate Peril Service Management.....	73
A.7.1.6.1.4 - Allocation and Retention Policy (ARP) Management.....	73
A.7.1.6.1.5 - Incident Command System (ICS) Service Management	73
A.7.1.6.1.5.1 - Real Time Priority & Role based QoS Development.....	73
A.7.1.6.1.6 - Processing of Responder Emergency Invocation	73
A.7.1.6.1.6.1 - Implementation of Immediate Location & Priority	73
A.7.1.6.2 - Enablement of Static User Profiles.....	74
A.7.1.7 - Payment Services Product Life Cycle Management	74
A.7.1.8 - Presence Services Product Life Cycle Management.....	74
A.7.1.8.1 - Local Status Update Provisioning	74
A.7.1.9 - Mobile Device Management Product Life Cycle Management.....	74
A.7.2 - User Services Portfolio Management.....	74
A.7.2.1 - Mission Critical Push to talk Voice (3GPP) Product Life Cycle Development & Management.....	74
A.7.2.1.1 - Security Management for Push to Talk Services	74
A.7.2.1.2 - Group Management/Communications Service Implement & Manage	75
A.7.2.2 - Broadcast Services Product Life Cycle Management	75
A.7.2.3 - Data Services Product Life Cycle Management	75
A.7.2.3.1 - Video Services Product Management	75
A.7.2.3.1.1 - Mobile Video Feeds Service Management.....	75
A.7.2.3.1.2 - 3rd Party Video Service Management.....	75
A.7.2.3.1.3 - Video Feeds Service Management	75
A.7.2.3.2 - CMAS Services Product Management.....	75
A.7.2.3.2.1 - Alert Aggregation Service Management	76
A.7.2.3.2.2 - Alert Dissemination Service Management.....	76
A.7.2.3.2.2.1 - Local Delivery Service Management	76
A.7.2.3.3 - Messaging Product Management	76

A.7.2.3.3.1 - Email Service Management	76
A.7.2.3.3.2 - Instant Messaging Service Management	76
A.7.2.3.3.3 - SMS/MMS Service Management.....	76
A.7.2.3.4 - M2M Feeds Product Management	77
A.7.2.3.4.1 - Mission Critical Data Service Management.....	77
A.7.2.3.4.2 - Non Mission Critical Data Service Management	77
A.7.2.3.5 - Cloud Services/Hosted Applications Management	77
A.7.2.3.5.1 - Manage Software as a Service (SaaS).....	77
A.7.2.3.5.2 - Manage Big Data Analytics Platform	77
A.7.2.3.5.3 - Manage Agency Information Homepage	77
A.7.2.3.5.4 - Manage Service Delivery and Installation	78
A.7.2.3.5.5 - Manage Infrastructure as a Service (IaaS).....	78
A.7.2.3.5.6 - Cloud Service Discovery Management	78
A.7.2.4 - Direct Mode Product Life Cycle Management	78
A.7.2.5 - Voice Services Product Life Cycle Management.....	78
A.7.2.5.1 - Cellular Telephony Product Management	78
A.7.2.5.1.1 - Call Forwarding Service Management.....	78
A.7.2.5.1.2 - Voice Mail Service Management.....	78
A.7.2.5.1.3 - Ring back tones Service Management	78
A.7.2.5.1.4 - Supplementary Service Management	79
A.7.2.5.1.4.1 - Directory Assistance Service Management.....	79
A.7.2.5.1.4.2 - Call Waiting Service Management	79
A.7.2.5.1.4.3 - Caller ID Service Management	79
A.7.2.5.2 - 9 1 1 Services Product Management.....	79
A.7.2.5.2.1 - E9 1 1 Service Management	79
A.7.2.5.2.1.1 - Text To 9 1 1 Service Management	79
A.7.2.5.2.2 - Provide Connection for NextGen 9 1 1 Service Management.....	80
A.7.3 - Security Requirements Management.....	80
A.7.4 - Public Safety Product, Feature Roadmap Development	80
A.7.4.1 - Develop Public Safety Product, Feature Roadmap.....	80
A.7.4.2 - Approve Public Safety Product, Feature Roadmap	80
A.7.5 - Product Management Support for FirstNet Industry Efforts	80
A.7.6 - Develop Offers (In Support of Sales)	80
A.7.6.1 - Develop Offers for Proposals.....	80
A.7.6.2 - Approve Offers for Proposals	80
A.8 - Stakeholder Management and Marketing	81
A.8.1 - Marketing Strategy	81
A.8.1.1 - Planning of the Marketing Strategy	81
A.8.1.2 - Conducting Market Research	81
A.8.1.3 - Defining Pricing Strategy	81
A.8.1.3.1 - Agreement with Provider(s) on Pricing Strategy.....	81
A.8.1.3.2 - Recommendation of Pricing Strategy.....	81
A.8.1.4 - Definition of Near Term Public Safety Product Roadmap	81
A.8.1.4.1 - Develop Near Term Public Safety Product Roadmap.....	81
A.8.1.4.2 - Approve Near Term Public Safety Product Roadmap	82
A.8.2 - Communications Strategy	82
A.8.2.1 - Public Affairs Communications Strategy	82

A.8.2.2 - Branding & Product Positioning Strategy	82
A.8.2.2.1 - Develop Branding & Product Positioning Strategy.....	82
A.8.2.2.2 - Approve Branding & Product Positioning Strategy	82
A.8.2.3 - Media Strategy Support	82
A.8.2.4 - Social Media Strategy Support	82
A.8.2.5 - Advertising & Promotion Strategy Support.....	82
A.8.2.6 - Community Relations Support	83
A.8.2.7 - Event Communications Support.....	83
A.8.3 - Market Analysis	83
A.8.3.1 - Segmentation Planning	83
A.8.3.2 - Customer Needs Analysis	83
A.8.3.3 - User Forecasting & Reporting	83
A.8.4 - PSAC Engagement.....	83
A.8.5 - Consultation	83
A.8.5.1 - State/Federal/Tribal Consultation.....	83
A.8.5.1.1 - Support Consultation Efforts	83
A.8.5.1.2 - Facilitate Resolution of Issues	84
A.8.5.1.4 - State/Federal/Tribal Outreach	84
A.8.5.1.4.1 - Events Management.....	84
A.8.5.1.4.2 - Events Management Support.....	84
A.8.5.2 - State Plan Development.....	84
A.8.5.2.1 - Pre State Plan Development Support.....	84
A.8.5.2.2 - Post State Plan Support.....	85
A.8.5.2.3 - Public Safety Stakeholder Data Collection & Analysis.....	85
A.8.5.2.4 - State Plan Change Management.....	85
A.8.5.2.5 - State Plan Delivery to Governor.....	85
A.8.5.3 - Governmental Affairs	85
A.8.5.3.1 - Direct Interaction with Congress.....	85
A.8.5.3.2 - Develop Federal/Congressional Outreach Plans.....	85
A.8.5.3.3 - Communication with Relevant Jurisdiction Committees	85
A.8.5.3.4 - Communication Development Across Federal Government	85
A.8.5.3.5 - Develop Hearing Testimonies.....	85
A.8.5.3.6 - Support States on FirstNet Related Items.....	86
A.8.5.3.8 - Support Local Governments on FirstNet related items.....	86
A.8.6 - User Fee Administration.....	86
A.8.6.1 - User Fee Determination with Contractor(s).....	86
A.8.6.2 - User Fee Implementation.....	86
A.8.6.3 - User Fee Approval Process Management with NTIA.....	86
A.8.7 - Definition of Device Portfolio	86
A.8.7.1 - Commercial Discussions/Negotiations for Devices & Pricing.....	86
A.8.7.2 - Device Embedded Apps Management	86
A.8.7.3 - Device Portfolio Strategy.....	86
A.8.7.3.1 - Develop Device Portfolio Strategy	86
A.8.7.3.2 - Approve Device Portfolio Strategy	86

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.

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.1.1.2 - Strategic Planning

Conduct strategic planning for FirstNet.

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 - Quality Assurance & 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 Oversight & Evolution

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 Compliance & Oversight

Responsible for defining and oversight of auditing NPSBN Key Performance Indicators to ensure contract compliance.

A.1.11.3 - Oversight of Prime Contractor's Network Performance Monitoring

Monitoring the overall NPSBN network performance. Identifying and resolving performance issues working with the contractors.

A.1.11.3.1 - Network Performance Analytics Oversight

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 - Oversee & Evolve 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 Oversight

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 - Oversight & Evolution 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 Policy Oversight

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.

A.1.13.2 - Network Identifiers Policy Oversight

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 Oversight

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 Oversight

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.1.13.4.1 - Oversight of RAN Border Design

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 Oversight & Approval

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 & Oversight

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 Approval

Definition of secondary use via CLAs use cases which will drive product requirements and network design guidelines.

A.1.15.3 - Other 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 Oversight

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 Oversight

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 Oversight

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 Oversight

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.1.18 - Customer Care Oversight & Performance Monitoring

Conduct customer care oversight and performance monitoring.

A.1.2 - Industry Relation Communications Oversight

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.1.2.5 - 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 Oversight

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.

A.1.3.2 - Spectrum Management Oversight

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 - NPSBN Economic Desirability Analysis Approval

Review and approve the economic desirability analysis done by the provider(s) for the rollout of the NPSBN.

A.1.3.6 - Monitor NPSBN 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 Oversight

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 Oversight & 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 Oversight of Marketing & Communications

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 - Opt Out States Oversight & Engagement

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 Oversight

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 - 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.2.1.2.2 - 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.2.1.2.3 - 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 - UE (User Equipment) 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 - Nationwide 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 polices and processes which need to be followed. The GSMA provides the IMEI Allocation and Approval Guidelines Version 6.0 27th July 2011, TS.06 (DG06) which FirstNet must follow.

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.2.1.3.1.1.3 - 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.2.1.3.1.2 - Policy, Apps & Content Administration

Administration of policies, applications and content on the devices of their users. Guidelines may be provided by FirstNet, prime contractor 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.2.1.3.1.3 - 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.2.1.3.1.4 - Diagnostics Monitoring and Administration

Administration of remote capture and data collection of customer devices. 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 and Administration

Management and administration of devices operating systems, firmware, and software. 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.2.1.3.1.5.1 - SW, OS & FW Management

Management of devices operating systems, firmware, and software. Guidelines for the proper device operating system, firmware & SW version and their updates may be provided by FirstNet, the prime contractor and device OEMs.

A.2.1.3.1.5.2 - SW, OS & FW Administration

Administration of devices operating systems, firmware, and software. Guidelines for the proper device operating system, firmware & SW version and their updates may be provided by FirstNet, the prime contractor 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 Administration

Administration of BOYD (Bring Your Own Device) configuration. Prime contractor and FirstNet will provide the necessary certified Mobile Device Management solution as part of the overall program.

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.

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.2.1.3.3.1.2.3.1 - Communications Groups Deactivation

Allows an agency to turn off the user or devices assignments to communications groups.

A.2.1.3.3.1.3 - User Administration: Provisioning of Users, User Profile Assignment, Rating (Billing) Activation

User provisioning administration via web-based tools (assign profiles, services, group subscriptions and billing). Prime contractor will provide the necessary web-based tools to provision users, assign profiles, assign appropriate billing alignment.

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

Administration of installation of specific local applications on devices or activation of specific services.

A.2.1.3.3.1.3.3.1 - Communications Groups Implementation

Administration of assignment of user or device 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.2.1.4.1 - View Agency Level Network Status

Monitoring network status, such as a local network operations center view for various agencies and/or states.

A.2.1.4.2 - 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.2.1.5.1 - Training on FirstNet Processes and Procedures

Training provider(s) in FirstNet specific processes and procedures.

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.2.1.5.3 - Training Users on Agency Specific Applications and Procedures

Training users in the usage of agency specific applications and procedures on FirstNet.

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.

A.2.1.6.2.1 - Develop Process for User Purchasing

Provide user purchasing processes for individually liable accounts.

A.2.1.6.2.2 - Approve Process for User Purchasing

Approve user purchasing processes for individually liable accounts.

A.2.1.6.3 - Provide Tier 1 Support

Provide web-based tools, access to call centers, processes, and systems to individually liable users to assist them with first level support.

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 - 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.2.3.1 - 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.2.3.2 - 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.

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.2.3.3 - Technical Strategy

Development and approval of long and short range roadmaps and strategy for the NPSBN.

A.2.3.3.1 - Develop Technical Strategy

Development of long and short range roadmaps and strategy for the NPSBN.

A.2.3.3.2 - Approve Technical Strategy

Approval of long and short range roadmaps and strategy 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.2.3.5 - Supply Chain Management Oversight

Oversight of all supply chain issues relating to systems engineering lifecycle activities.

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 Review 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 - 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.3.2.5 - 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.

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.

A.3.4.1 - Long Term Feature, Function, and Technology 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 the needs of Public Safety users and new customer demand.

A.3.4.1.1.1 - Approve Test and Trial Recommendation

Approve or reject Prime Contractor's recommendations for test, trial, and/or deployment of new services, features, and technology.

A.3.4.1.1.2 - Perform Research, Test, and Trial of New Technology, Service, and Features

Research, prototype, test, and trial new services, features, and technology (Core/RAN/Device) to determine viability for deployment, potential uses, functional value and ensure FirstNet remains synchronized with the applicability of industry developments and standards.

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.3.4.1.1.6 - Participation & Approval of Proof of Concept & Field 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.3.4.1.2.1.1 - Sales Feedback for Long Term Services

Sales feedback and requirements gathering for development of three year+ and beyond public safety product roadmap.

A.3.4.1.2.1.2 - Outreach Feedback for Long Term Services

Outreach feedback and requirements gathering for development of three year+ and beyond public safety product roadmap.

A.3.4.1.2.2 - Feature & Services Roadmap Development

Identify system features and services in support of the long term product development roadmap.

A.3.4.1.2.2.1 - Integrate Features & Services into Long term NPSBN Roadmap

Determine pre-decisional position on the integration of products, as identified, into the long term NPSBN roadmap.

A.3.4.1.2.2.2 - Standards Roadmap Development for Public Safety

Drive Standards organizations to implement the FirstNet long term roadmap.

A.3.4.1.3 - Long Term Feature Feasibility Analysis

Provide feasibility analysis for feature planning. Assess the financial and technical feasibility of the new offered or required feature or function for FirstNet.

A.3.4.1.4 - Supplier Roadmap Coordination

Interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.

A.3.4.1.5 - Global and US Standards Participation, Alignment and Collaboration

This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.

A.3.4.1.5.1 - Global and US Standards Strategy – Approval of final strategy and tactics

This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.

A.3.4.1.5.2 - Global and US Standards Strategy, Develop Strategy and propose to FirstNet

This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.

A.3.4.1.5.3 - Global and US Standards Participation – FirstNet, Prime Vendor, and FirstNet/Vendor’s Ecosystem Partners

This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.

A.3.4.1.5.3.1 - FirstNet Participation

This function will interface and coordinate with provider(s) to ensure FirstNet's feature requirements and items are included in provider(s) releases.

A.3.4.1.5.3.2 - Prime Contractor and FirstNet EcoSystem Participation

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.3.4.2.2 - 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.3.4.2.2.1 - Mission Critical PTT Engineering & Design

Engineer and design mission critical push to talk services as defined by product management.

A.3.4.2.2.2 - Group Communications Engineering & Design

Design and engineer group communications services, as defined by product management.

A.3.4.2.2.4 - Location Platform Engineering & Design

Design and engineer location based services, as defined by product management.

A.3.4.2.2.5 - IMS Platform Engineering & Design

Design and engineer IMS based services, as defined by product management (e.g VoLTE, identity management, presence, IP messaging, 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.

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 & Design

Design and engineer Multicast platforms required to support eMBMS services, as defined by product management.

A.3.4.2.2.7 - Mobile Device Management Systems Engineering & Design

Design and engineer the device management system and network control platform(s), to support device management services on the NPSBN.

A.3.4.2.2.7.1 - Multi-Tenant Management Engineering & Design

Design and engineer a device management solution that supports multi-tenant control functionality ("multi-tenant control" describes the ability of multiple device managers to have simultaneous access, for device management).

A.3.4.2.2.7.10 - Mobility Management Systems Engineering & Design

Design and engineer the device management functionality required to support sending of mobility management related updates to mobile devices.

A.3.4.2.2.7.2 - Policy & Content Management Engineering & Design

Design and engineer the device management system 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 - Over The Air (OTA) Updates Engineering & Design

Design and engineer 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 - Mobile Diagnostics, Polling, & Reporting Tools Engineering & Design

Design and engineer the management tools required to support polling of diagnostic and reporting measures from FirstNet mobile devices (e.g. device problems, network performance).

A.3.4.2.2.7.5 - Software, OS, & Firmware Management Tools and Processes Engineering & Design

Design and engineer the operating system, software, and firmware management system. This includes the capability of polling, notifying, and updating all devices in the FirstNet device portfolio connected to the FirstNet system by OTA, tethered, or roaming, including Wi-Fi connectivity, to have its operating system, software, and firmware version determined, updated, and verified, as needed.

A.3.4.2.2.7.6 - Tethered Device Updates Engineering & Design

Design and engineer 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 - Configuration Management Tools and Systems Engineering & Design

Design and engineer device configuration management tools and systems. This includes the capability of polling & updating all devices in the FirstNet device portfolio.

A.3.4.2.2.7.8 - BYOD Tools and Methods Enablement Engineering & Design

Design and engineer 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 - UICC/SIM Management Engineering & Design

Design and engineer systems required to manage SIMs and UICC profiles for network configurations, roaming provider(s), and other necessary applications.

A.3.4.2.2.8 - Direct Mode Communications 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.3.4.2.3.2 - 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 Architecture & 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 Planning & 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.

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 - 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.

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.

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 Develop/Implement platforms and Systems

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 Develop/Implement platforms and Systems

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 - Billing Profiles Develop and Implement

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.

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 peps 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 and Implementation

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: 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 including Lab 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 in Lab

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 - Lab 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

Conduct 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

Conduct software updates (including major and point releases) across multiple network elements. Coordinate and teste 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 physical (hardware or facility replacement/repair) and software/translation related modifications required to restore service to full user functionality.

A.3.8.2.2.3 - Equipment Spares Management

Management 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 - Manage Network Operations

Manage the configuration, optimization, and implementation of the NPSBN

A.3.8.2.3.1 - Manage Network, Roaming, and Identifier Configuration

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) Implementation

Manage the authorization, execution, and operation of all CALEA requirements for the NPSBN including but not limited to location tracking, cyber monitoring, signalling intercept, voice intercept, data intercept, and messaging intercept.

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 - Management Network Element, Software, and Feature Releases

Manage software, hardware, and feature updates (minor and major releases) across all NPSBN network elements.

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.

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 - Perform Device Mobility Management

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 device configuration and updates

Management and operation of device diagnostics, polling, and reporting tools for device software, OS, and firmware via tethering and/or over-the-air (OTA) methodology.

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 Support and Reporting

Diagnosing and reporting of service impairments to resolve issues in the most expeditious manner possible. Engagement of Tier 1, 2, and 3 resources 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 - Provide technical support for issue resolution

Provide a tiered technical support structure for efficient resolution of NPSBN issues. Support tiers are focused on network monitoring, alarming, and reporting (including resource dispatch) to resolve network impairments. Tiered structure supports escalation paths to higher levels as technical complexity dictates.

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

Identification of network or service fault or performance degradation and implementation of 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

Identification of root causes and 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

Review of recommendations and implementation across all services for applicability to reduce further risk of problem reoccurrence.

A.3.8.2.3.7 - Administer Local Control System

Administer the local control architecture including user/group profiles and device profiles.

A.3.8.2.3.7.1 - Administer and Maintain Local Control User Service

Administer the local agency user/group profile, device profile, and associated services. Coordinate local control portal and administration issues with appropriate agencies.

A.3.8.2.3.7.1.1 - Develop guidelines for Static and Dynamic Profiles

Develop and manage the operational guidelines 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.3.8.2.3.7.1.2 - Develop Guidelines for NIMS ICS

Implement and manage the policy and governance guidelines of national incident management (NIMS ICS Types 1, 2, 3, 4, 5) protocols and processes with FirstNet and other federal/local agencies.

A.3.8.2.3.7.2 - Develop Local Control User Operations Guidelines

Develop guidelines to support network monitoring, provisioning, QPP provisioning, and accounting.

A.3.8.2.4 - Perform Quality Assurance, Testing, and Certification

Perform the overall testing for all network elements and devices to ensure compatibility and performance specifications are met on the NBPSN.

A.3.8.2.4.1 - Design, execution, and acceptance of user equipment carrier tests

Manage and conduct device planning, testing, and certification for 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

Manage and conduct required tests to validate device performance and interoperability requirements 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

Manage and conduct device application interoperability tests to ensure device applications meet performance requirements.

A.3.8.2.4.1.4 - Manage User Equipment FCC and PTCRB Certification

Provide appropriate test suites to ensure that devices are authorized and certified as FCC and PTCRB compliant. 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.3.8.2.4.1.4.2 - 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.3.8.2.4.1.5 - Device Administration of Secondary User via CLA

Manage administration of devices used by secondary users to ensure proper access to the NPSBN.

A.3.8.2.4.2 - Field Test Execution

Execution of field testing for major software upgrades and new services prior to activation 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 - Execution of 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 - Execution of Opt out RAN Interconnection testing

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 - Execution of 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 - Execution of Roaming Interconnection Testing

Execution of 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 - Execution of Inter carriers Interconnection Testing

Execution of 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

Execution of interconnection testing for trusted and non-trusted non-3GPP connections between FirstNet's core network and the core network and other wireless operators for delivery of data and voice services.

A.3.8.2.4.3.5 - Execution of Backhaul & Backbone Interconnection Testing

Execution of tests for microwave, fiber, satellite and cable systems layers 1, 2, and 3 including all failover links related to cell site-core and core-core connectivity to ensure all quality NPSBN quality metrics are met.

A.3.8.2.4.3.6 - Execution of PSEN Interconnection Testing

Execution of tests for connections and routing between NPSBN and the PSENs to validate APN connections to PSEN and mobile VPNs.

A.3.8.2.4.3.7 - Execution of Cloud Services Interconnection Testing

Execution of tests for connections between the NPSBN and cloud services. Examples service include video, telepresence and desktop endpoint type testing to ensure a seamless and consistent experience from the user's perspective.

A.3.8.2.4.4 - Perform Application Certification

Perform certification of NPSBN application based on FirstNet defined test and certification processes to ensure 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.

A.3.8.2.4.4.1 - Perform 3rd Party Sandbox Certification

Perform certification testing of applications withing a Pre-certification or Sandbox environment for very limited users. Function includes management of 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 - Perform FirstNet Hosted Application Certification

Perform application certification to validate the system level testing on Pre-Production environment for friendly users in Live environment.

A.3.8.2.4.5 - Perform NPSBN System Integration Testing

Perform integration of all nodes within the NPSBN in the lab to ensure the network functions normally. NPSBN nodes include but are not limited to Device Manager Platform, RAN, EPC, BSS, and Application Delivery Platform.

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 - Manage Service Experience

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.

A.3.8.2.4.6.1 - Perform Service Experience Data Analytics

Provide usage, location, and performance data analytics in support of Service Experience Management related to NPSBN 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 - Manage Service Availability

Ensure that NPSBN systems are operating according to design in order 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 - Manage Service Capacity

Ensure that NPSBN services are operating within the designed capacity to meet current and immediate future business capacity needs.

A.3.8.2.4.6.4 - Manage Service Level

Ensure that NPSBN KPIs are properly identified and measured in order to meet or exceed end user quality guidelines.

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.

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.3.8.2.5.3.2 - 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 - Security Policy Enforcement

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.3.8.2.5.4.1 - Public Safety Agency Policy Enforcement

Ensure public safety agencies comply with FirstNet's security polices and procedures to prevent potential security breaches.

A.3.8.2.5.4.2 - Federal Security Policy Enforcement

Ensure federal agencies comply with FirstNet's security polices and procedures to prevent potential security breaches.

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

Restore network from service impairments involving any aspect 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 - NPSBN 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 - NPSBN Mitigation Implementation

Mitigation plans will be implemented as required on site during events and as part of simulated (training) events.

A.3.8.2.6.6.2 - Agency Support for NPSBN 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.3.8.2.6.7 - 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 - Perform Network Monitoring

Manage and operate the tools and services required 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 - Manage Network Operations Center

Provide a National Network Operations Center to provide 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 - Manage Trouble Ticket Process

Provide a trouble ticketing system 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 - Manage Network Issues

Manage network events which may 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.

A.3.8.3.2 - Manage Agency Security Operations Center

Establish and maintain protocols working with FirstNet and Agency SOC's to ensure agency applications and data remain secure.

A.3.8.3.2.1 - Manage Intrusion Protection System

Provide an intrusion protection system to allow proactive and real-time sampling of both internal and network traffic. Review and provide logs to detect and eliminate in-progress and future threats.

A.3.8.3.2.2 - Perform Intrusion Recovery Procedures

Manage procedures related to 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 - Manage Federal Security Operations Center

Manage communications between the federal security operations center and the NPSBN security center.

A.3.8.3.4 - Manage NPSBN Security Operations Center

Provide monitoring, detecting, and resolution of incidents that may affect the confidentiality, integrity, or availability of network devices, end-user devices, and systems.

A.3.8.3.4.1 - Perform NPSBN Security Intrusion Monitoring & Detection by SOC

Provide surveillance and identification when an unauthorized access attempt has been made, is occurring, or has occurred.

A.3.8.3.4.2 - Perform Device Malware Detection and Deletion

Provide 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 & Procedures

Define policies and procedures focused on business processes related to provisioning, billing, certification, profiles, deployment and operational guidelines.

A.4.1 - Define, Implement, and Monitor Provisioning Policies & Procedures

Develop, implement, and monitor the provisioning policies and procedures relating to subscription management of agencies and users.

A.4.1.1 - Define and Implement Provisioning Procedures

Define and implement the provisioning policies and procedures through coordination with FirstNet and their subsequent consultation with their stakeholder community.

A.4.1.2 - Monitor Provisioning Policy & Procedure Compliance

Monitor, enforce, and provide feedback on the provisioning policies and procedures implemented by the Prime Contractor.

A.4.10 - Implement and Enforce Policy Procedures Across Local Public Safety Entities

Implement and enforce security policies, business processes, and operational procedures within the local public safety community.

A.4.2 - Define, Implement, and Monitor Network Policies & Procedures

Develop, implement, and monitor overall network operating policies and procedures for the NPSBN. Enforce all laws, rules, standards, and regulations under FirstNet's purview.

A.4.2.1 - Define and Implement Operational Procedures

Define operational procedures to be implemented throughout the NPSBN. These procedures will provide guidance to field teams on the methods to achieve optimal network performance and meet all NPSBN statutory requirements.

A.4.2.2 - Monitor Operational Procedure Compliance

Monitor, enforce, and provide regular feedback to support the improvement of network operating procedures.

A.4.3 - Define Standard Definitions for Static QPP, Dynamic QPP, and User Subscription profiles

Develop the user policy profile framework specifically for static (non-emergency), dynamic (emergency), and user subscription profiles (i.e. voice, data, and push-to-talk).

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.4.4 - Define, Implement, and Monitor Billing Policies & Procedures

Define the policies and procedures relating to billing subscriptions, rate plans, and both home and roaming scenarios. Oversight of this function will be executed through A.1.17 – Sales Management Oversight and Performance Monitoring.

A.4.5 - Security and Network Operations Best Practices

Develop best practices for security, industry standards on processes, and network and business operations.

A.4.5.1 - Develop Security and Network Operations Best Practices

Develop best practices for security and network operations incorporating agency and key state learnings.

A.4.5.2 - Approve Security and Network Operations Best Practices

Approve for implementation of best practices for security and network operations.

A.4.6 - Develop Customer Care Policies & Procedures

Develop policies and procedures to support the care of users, including account management, resolving user issues, and billing. Oversight of this function will be executed through A.1.6 – Stakeholder Management and Marketing.

A.4.7 - Develop Marketing Policies & Procedures

Develop and manage marketing policies and procedures in consultation with state and local governments, tribal nations and territories, and public safety entities. Oversight of this function will be executed through A.1.6 – Stakeholder Management and Marketing.

A.4.8 - Develop Sales Policies & Procedures

Develop and manage sales policies and procedures in consultation with the Prime Contractor, state and local governments, tribal nations and territories, and public safety entities. Oversight of this function will be executed through A.1.17 – Sales Management Oversight and Performance Monitoring.

A.4.9 - System Engineering Oversight of Policies & Procedures

Oversee system engineering within the NPSBN to enforce compliance of the engineering lifecycle and evolution of the NPSBN.

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.

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 - NPSBN 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

Develop and implement a sales strategy framework for public safety devices, services and applications

A.6.1 - Public Safety Entity Sales Channel Management

Develop and execute overall sales targets and performance for devices, services and applications

A.6.1.1 - Public Safety Sales

Develop and execute targets for sales and service performance for public safety agencies (including: law enforcement, fire departments, EMS services, 911 service centers, and other public safety entities) and solicit inputs on evolving requirements for devices, services and applications

A.6.1.1.1 - Law Enforcement Sales

Develop and execute targets for sales and service performance for local law enforcement agencies and solicit inputs on evolving requirements for devices and services

A.6.1.1.2 - Fire Department Sales

Develop and execute targets for sales and service performance for local fire departments and solicit inputs on evolving requirements for devices, services and applications

A.6.1.1.3 - EMS Sales

Develop and execute targets for sales and service performance for local EMS agencies and solicit inputs on evolving requirements for devices, services and applications

A.6.1.1.4 - 911 Sales

Develop and execute targets for sales and service performance for local 911 service centers and solicit inputs on evolving requirements for devices, services and applications

A.6.1.1.5 - Others Entity Sales

Develop and execute targets for sales and service performance for other public safety entities and solicit inputs on evolving requirements for devices, services and applications

A.6.1.2 - Federal Sales

Develop and execute targets for sales and service performance for Federal Government agencies (Public Safety and Non Public Safety) and solicit inputs on evolving requirements for devices, services and applications

A.6.1.2.1 - Federal Public Safety Sales

Develop and execute targets for sales and service performance for Federal Public Safety agencies and solicit inputs on evolving requirements for devices, services and applications

A.6.1.2.2 - Federal Non Public Safety Sales

Develop and execute targets for sales and service performance for Federal Non Public Safety agencies and solicit inputs on evolving requirements for devices, services and applications

A.6.1.3 - State Government and Tribal Sales

Develop and execute targets for sales and service performance for State Government and Tribal organizations (Public Safety and Non Public Safety) and solicit inputs on evolving requirements for devices, services and applications

A.6.1.3.1 - State Government and Tribal Public Safety Sales

Develop and execute targets for sales and service performance for State Government and Tribal public safety organizations and solicit inputs on evolving requirements for devices, services and applications

A.6.1.3.2 - State Government and Tribal Non Public Safety Sales

Develop and execute targets for sales and service performance for State Government and Tribal non public safety organizations and solicit inputs on evolving requirements for devices, services and applications

A.6.1.4 - Retail Sales

Establish and operate retail distribution channels (both direct and through 3rd parties) that facilitate user acquisition and customer sales activities.

A.6.1.4.1 - Retail/Provider(s) Sales

Responsible for sales activities and user acquisition within the offeror(s) retail sales channel.

A.6.1.4.2 - Retail/3rd Party Sales

Responsible for sales activities and user acquisition within the 3rd party sales channel.

A.6.1.5 - Internet and Telemarketing Sales

Establish and operate alternative sales channels, including Internet and inbound/outbound telemarketing, to facilitate user acquisition, conduct customer sales activities, and solicit inputs on evolving requirements for devices, services and applications.

A.6.1.6 - Utility Responder Sales

Establish and operate sector sales channels focused on Utility Responder sales and evolving requirements for devices, services and applications.

A.6.1.6.1 - Sales to Utilities

Responsible for working with utility sales channels on sales and evolving requirements for devices, services and applications.

A.6.1.7 - Account Management

Responsible for the strategy and execution of account management functions, including, but not limited to pre and post sales and marketing activities.

A.6.1.7.1 - Customer Acquisition Planning & Implementation

Responsible for the strategy and execution of customer acquisitions through promotions, sales channels, and collateral.

A.6.1.7.2 - Customer Retention/Winback Planning and Implementation

Responsible for the strategy and execution 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 functions.

A.6.1.7.3.1 - Conduct Account Planning

Develop the strategy for account planning regarding sales and on-going account management functions.

A.6.1.7.3.2 - Account Planning Compliance

Monitor account planning strategy for compliance regarding sales and on-going account management functions.

A.6.1.7.4 - Special Pricing Development

Development of special pricing offers for custom solutions and/or high volume opportunities.

A.6.1.8 - User Migration and Evolution

Support 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

Develop the framework and processes required for an efficient sales operation and support service functionality

A.6.2.1 - Sales Reporting

Monitor and produce management reports on the performance of sales channels, reporting on all KPIs as required.

A.6.2.2 - Compensation Planning and Implementation

Develop and implement a competitive sales channel compensation strategy

A.6.2.3 - Sales Training

Develop and implement a FirstNet-specific sales training program

A.6.2.4 - Service Fulfilment

Develop and implement process to ensure fulfilment of services, devices and applications for all NPSBN customers

A.6.3 - Sales Planning

Develop sales plans for all segments of NPSBN customers

A.6.3.1 - Sales Strategy and Compliance

Develop the strategic framework for the successful implementation of the sales plans for all segments of customers and monitor its performance.

A.6.3.1.1 - Identify priority elements of Sales Strategy

Identify priorities for the strategic framework to implementat the sales plans for all segments of customers and monitor its performance.

A.6.3.1.2 - Develop Sales Strategy

Develop the strategic framework for the successful implementation of the sales plans for all segments of customers and monitor its performance.

A.6.3.1.3 - Approve Sales Strategy

Approve 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 short and long term sales forecasts and adjust according to changing market trends and dynamics.

A.6.3.2.1 - Sales Targets and Monitoring Performance

Develop short and long term sales forecasts and adjust according to changing market trends and dynamics. Measure target performance achievements

A.6.3.2.2 - Sales Results Reporting/Trends

Execute, monitor, and report sales performance to meet short and long term sales forecasts.

A.6.3.3 - Sales Monitoring and Compliance

Develop a standard sales performance monitoring framework and ensure timely distribution and review of sales reports

A.6.4 - Major Accounts Management

Develop and implement strategies to acquire and service major accounts, including account monitoring and high level management reports on major accounts performance

A.6.5 - Sales Engineering Support

Provide customized engineering and go to market support for major accounts and projects

A.6.5.1 - Facilitate Product Demonstrations

Develop and implement processes that facilitate the demonstration of products, services and applications 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 support for sales proposals and special projects

A.6.5.4 - Provide Product Feedback to Engineering

Collect and provide information on technical and operational issues to engineering and product management staff

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.

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.7.1.4.2.1 - Identity 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.7.1.4.2.2 - 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.

A.7.1.4.2.2.1 - Defining 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.

A.7.1.4.2.2.2 - Approve 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.

A.7.1.4.3 - Define and Support Access Policies

Access Policies are used by the Authorization Services and provide the access constraints, rules and details for applications, services and resources. Access Policies are dynamic and can be created, updated and removed. Access policies can be shared across multiple resources, and should be standardized and normalized for FirstNet where possible. An example of a standardized access policy would be one written in extensible Access Control Markup Language (XACML). A standardized format for access policies should be used so they can easily be validated and shared by different resources. The applications and services provided by local agencies must make use of these policies. Agencies must be able to tailor these policies for applications and services for which they have local control.

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.7.1.4.3.2 - 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.7.1.4.4 - Manage Authorization Services

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.

A.7.1.4.5 - Manage Authentication Services

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.

A.7.1.4.5.1 - Manage Multi Factor Authentication

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.

A.7.1.4.5.2 - Manage Single Sign on

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.

A.7.1.5 - Group Communication (GCSE 3GPP) Product Life Cycle Management

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.

A.7.1.6 - QoS, Priority, and Preemption (QPP) Administration

Defines, plans, obtains the acceptance for the QoS, Priority, and Preemption mechanisms. Centralized authorization, identity management, and subscriber information and QoS, Priority, and Preemption policies would be employed to manage the distribution of control across the agency/FirstNet touch points.

A.7.1.6.1 - Management and Enablement of Dynamic User Profiles

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.

A.7.1.6.1.1 - Management of Access Class Barring

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.

A.7.1.6.1.2 - Management of QoS Class Identifiers (QCI)

Enable and support of all 9 QCI classes specified in table 6.1.7 of 3GPP 23.203 v9.11 or future equivalents.

A.7.1.6.1.3 - Immediate Peril Service Management

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).

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 Development

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 - 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 GSMA Rich Communications recommendations (RCS) and aggregate and deliver real time presence information including user availability, service capability, and social presence for associated public safety contacts and groups across FirstNet.

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 Development & 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 Implement & Manage

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.

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.7.2.3.1.3 - 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.

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.

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").

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.7.4 - 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.7.4.1 - Develop Public Safety Product, Feature Roadmap

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.7.4.2 - Approve Public Safety Product, Feature Roadmap

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.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.8.1.3.1 - 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.8.1.3.2 - Recommendation of Pricing Strategy

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

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.8.1.4.1 - Develop Near Term Public Safety Product Roadmap

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.8.1.4.2 - Approve Near Term Public Safety Product Roadmap

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.8.2.1 - 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.8.2.2 - 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.8.2.2.1 - Develop 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.8.2.2.2 - Approve 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 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.

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.8.4 - PSAC Engagement

PSAC Engagement involves meeting planning and execution and administrative services of the PSAC, its subcommittees, and working group.

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.8.5.1.2 - 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 - 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.8.5.1.4.1 - 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.8.5.1.4.2 - 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: 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

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.8.5.2.3 - 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 - Develop 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 - 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.8.6.3 - 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 - 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.

A.8.7.3 - Device Portfolio Strategy

Define the range of device/accessories types to cover all Public Safety service requirements including pricing.

A.8.7.3.1 - Develop Device Portfolio Strategy

Define the range of device/accessories types to cover all Public Safety service requirements including pricing.

A.8.7.3.2 - Approve Device Portfolio Strategy

Define the range of device/accessories types to cover all Public Safety service requirements including pricing.