



# Appendix C-9

## Nationwide Public Safety Broadband Network (NPSBN) Use Case Definitions

*Special Notice D15PS00295 – Nationwide Public  
Safety Broadband Network (NPSBN)*

04/27/2015

## Table of Contents

<b>1</b>	<b>Document Overview.....</b>	<b>1</b>
<b>2</b>	<b>Use Case Description.....</b>	<b>1</b>
2.1	Use Case ID .....	1
2.2	Use Case Name .....	1
2.3	Description.....	1
2.4	Actors.....	1
2.5	Pre-conditions.....	1
2.6	Post-conditions .....	1
2.7	Frequency of Use .....	2
2.8	Normal Course of Events .....	2
2.9	Alternative Courses.....	2
2.10	Exceptions.....	2
2.11	Includes.....	2
2.12	Special Requirements .....	2
2.13	Assumptions.....	2
2.14	Operational Architecture Referenced Functions.....	2
<b>3</b>	<b>Use Case Inventory.....</b>	<b>3</b>
<b>4</b>	<b>Use Cases .....</b>	<b>4</b>
4.1	Incidents.1: FEMA Type 1: National.....	4
4.2	Incidents.2: FEMA Type 2: Regional.....	4
4.3	Incidents.3: FEMA Type 3: Multi-jurisdictional.....	4
4.4	Incidents.4: FEMA Type 4: Terrorist Surveillance .....	4
4.5	Incidents.5: FEMA Type 5: Traffic Stop .....	4
4.6	Events.1: Major Planned Event.....	4
4.7	Customer Lifecycle.1: Agency On-boarding and Lifecycle Support .....	4
4.8	Local Control.1: Services, Applications, User, and Device Management .....	9
4.9	Local Control.2: Network Operations and Maintenance .....	22
4.10	QPP.1: Quality of Service, Priority, and Preemption (QPP) .....	22
4.11	QPP.2: Dynamic QPP Management .....	33
4.12	User Services.1: Mission-Critical Services.....	33
4.13	User Services.2: Proximity Services .....	33
4.14	User Services.3: Cloud Services.....	33
4.15	User Services.4: Secondary Users .....	33
4.16	Network Services.1: Services Delivery Platform (SDP) .....	34
4.17	Network Services.2: Public Safety Enterprise Network (PSEN) Interconnect.....	34
4.18	Network Services.3: Regulatory Services.....	39
4.19	Devices.1: Device Ecosystem .....	39
4.20	Devices.2: Mobile Device Management (MDM).....	39
4.21	Devices.3: Bring Your Own Device (BYOD) .....	39
4.22	Devices.4: Mobile Communications Unit (MCU) .....	44
4.23	Applications.1: Identity, Credential and Access Management (ICAM).....	44
4.24	Applications.2: Application Development Lifecycle.....	44
4.25	Applications.3: App Stores: FirstNet, Local, Commercial.....	45

4.26	Security.1: Rogue App, Malware Detection and Mitigation .....	47
4.27	Security.2: PSEN Threat Detection and Exclusion.....	47
4.28	Operations.1: Network Management.....	47
4.29	Operations.2: Network Operations Center (NOC).....	48

## List of Tables

Table 1	Use Case Inventory.....	3
Table 2	Customer Life Cycle.1 References to Operational Architecture .....	9
Table 3	Local Control Definition.....	10
Table 4	Local Control.1 Operational Architecture References .....	21
Table 5	QPP1, M2M, Secondary Users.4 Operational Architecture References .....	32
Table 6	Network Services.2 Operational Architecture References .....	38
Table 7	Devices.3 Operational Architecture References .....	43
Table 8	Applications.3 Operational Architecture References.....	47

DRAFT

## 1 Document Overview

In order to meet FirstNet's program objectives, FirstNet will rely on a set of illustrative use cases. One of the objectives of this document is to illustrate usage of the main functions of FirstNet as defined in the Appendix C-7, Operational Architecture. Where appropriate, references are provided to the functions in the Operational Architecture.

In this draft, the content is largely limited to the list of use cases, their titles, and a brief description of each. In addition, a few detailed examples have been included which will serve to illustrate how all of the completed use cases will ultimately be incorporated.

## 2 Use Case Description

Each use case is presented using the following format.

### 2.1 Use Case ID

Each use case has a unique identifier, in hierarchical form: <use case segment>.X, where X is the use case number. Related use cases are grouped in use case segments, for example Incidents.1 through Incidents.5.

### 2.2 Use Case Name

A concise, results-oriented name is provided for each use case. These reflect the tasks the user needs to be able to accomplish using the system, including an action verb and a noun.

### 2.3 Description

Each use case has a brief description of the reason for and outcome of this use case, or a high-level description of the sequence of actions, and the outcome of executing the use case.

### 2.4 Actors

An actor is a person or other entity external to the system being specified that interacts with the system and performs actions within the use case to accomplish tasks. Different actors often correspond to different user classes, or roles, identified from the public safety community that will use the product. The actor(s) that will be performing this use case are named, for example, Fire Fighter, Incident Commander, secondary users, and the provisioning system.

### 2.5 Pre-conditions

Pre-conditions are a list of activities that must take place, or any conditions that must be true, before the use case can be started.

### 2.6 Post-conditions

These are descriptions of the state of the system at the conclusion of the use case.

## 2.7 Frequency of Use

This is an estimate of the number of times this use case will be performed by the actors per some appropriate unit of time, such as, continuously, hourly, daily, weekly, or monthly.

## 2.8 Normal Course of Events

A detailed description of the user actions and system responses that will take place during execution of the use case under normal, expected conditions is provided. This dialog sequence will ultimately lead to accomplishing the goal stated in the use case name and description.

## 2.9 Alternative Courses

Other potential usage scenarios that can take place within this use case.

## 2.10 Exceptions

Exceptions are any anticipated error conditions that could occur during execution of the use case, along with a definition of how the system is to respond to those conditions. Also described is how the National Public Safety Broadband Network (NPSBN) is to respond if the use case execution fails for some unanticipated reason.

## 2.11 Includes

This is a list of any other use cases that are included (“called”) by this use case.

## 2.12 Special Requirements

Special requirements are any additional requirements, such as non-functional requirements, for the use case that may need to be addressed during design or implementation. These requirements may include performance, capacity, or other quality attributes.

## 2.13 Assumptions

Assumptions are a list of assumptions that were made in the analysis that might influence the use case description, pre-conditions, post-conditions, or normal course of events.

## 2.14 Operational Architecture Referenced Functions

A cross-reference between this use case and the functions in the Operational Architecture, Appendix C-7 which have been included in the use case is provided.

### 3 Use Case Inventory

Table 1 Use Case Inventory

Use Case #	Use Case ID	Use Case Name
UC 1	Incidents.1	FEMA Type 1: National
UC 2	Incidents.2	FEMA Type 2: Regional
UC 3	Incidents.3	FEMA Type 3: Multi-jurisdictional
UC 4	Incidents.4	FEMA Type 4: Terrorist Surveillance
UC 5	Incidents.5	FEMA Type 5: Traffic Stop
UC 6	Events.1	Major Planned Event
UC 7	Customer Lifecycle.1	Agency On-boarding and Lifecycle Support
UC 8	Local Control.1	Services, Applications, User, and Device Management
UC 9	Local Control.2	Network Operations and Maintenance
UC 10	QPP.1	Quality of Service (QoS), Priority, and Preemption (QPP)
UC 11	QPP.2	Dynamic QPP Management
UC 12	User Services.1	Mission-Critical Services
UC 13	User Services.2	Proximity Services
UC 14	User Services.3	Cloud Services
UC 15	User Services.4	Secondary Users
UC 16	Network Services.1	Services Delivery Platform (SDP)
UC 17	Network Services.2	Public Safety Enterprise Network (PSEN) Interconnect
UC 18	Network Services.3	Regulatory Services
UC 19	Devices.1	Device Ecosystem
UC 20	Devices.2	Mobile Device Management (MDM)
UC 21	Devices.3	Bring Your Own Device (BYOD)
UC 22	Devices.4	Mobile Communications Unit (MCU)
UC 23	Applications.1	Identity, Credential and Access Management (ICAM)
UC 24	Applications.2	Application Development Lifecycle
UC 25	Applications.3	App Stores: FirstNet, Local, Commercial
UC 26	Security.1	Rogue App, Malware Detection and Mitigation
UC 27	Security.2	PSEN Threat Detection and Exclusion
UC 28	Operations.1	Network Management
UC 29	Operations.2	Network Operations Center (NOC)

## 4 Use Cases

### 4.1 Incidents.1: FEMA Type 1: National

This use case describes a scenario from the SAFECOM, NPSTC, or Public Safety Advisory Committee (PSAC) use cases where a Federal Emergency Management Agency (FEMA) Type 1 incident has transpired. This use case illustrates a scenario with a wide scope of loss of commercial wireless services and the use of deployables, Mobile Communications Units (MCU), and other range extension solutions to provide coverage and capacity in support of Incident Command Structure (ICS) and National Incident Management Systems (NIMS) support needs.

### 4.2 Incidents.2: FEMA Type 2: Regional

This use case describes a scenario from the SAFECOM, NPSTC, or PSAC use cases, where a FEMA Type 2 incident has transpired, specifically including deployables, MCU, and other range extension solutions. It demonstrates the capacity metrics associated with a deployable as well as the need for geographical distribution.

### 4.3 Incidents.3: FEMA Type 3: Multi-jurisdictional

This use case describes a scenario from the SAFECOM, National Public Safety Telecommunications Council (NPSTC), or PSAC use cases, where a FEMA Type 3 incident has transpired. Another FEMA Type 3 scenario is also included in the SAFECOM Type 3 Explosion use case for QPP.1.

### 4.4 Incidents.4: FEMA Type 4: Terrorist Surveillance

This is a NPSTC use case which includes a variety of federal and local agencies and their interactions during the field surveillance of a terrorist suspect.

### 4.5 Incidents.5: FEMA Type 5: Traffic Stop

This is a SAFECOM use case involving a Type 5 incident of a routine traffic stop.

### 4.6 Events.1: Major Planned Event

This use case is a pre-planned major event, such as a state fair, National Football League football game, or the Sturgis Rally, where a number of users from different agencies have to manage potential network congestion due to the location and crowds. Capacity is augmented through the use of deployables, and additional security assets such as surveillance cameras are pre-positioned for the event(s).

### 4.7 Customer Lifecycle.1: Agency On-boarding and Lifecycle Support

This use case includes new agency training, security, subscription management, user administration, device administration, identity administration, migration from other carriers, and impacts of state opt-out. Agencies include police, fire, Emergency Medical Services, and secondary responders.

### 4.7.1 Description

An agency needs to be on-boarded to the NPSBN to allow the agency's end users to access local agency applications such as dispatch, email, and agency developed applications as well as federal services such as the International Justice and Public Safety Network (NLETS) in a secure and fast manner. The use cases describe some of the administrative processes and procedures for managing user accounts, their devices, and resolving issues the end-users may have. Broadly, customer lifecycle management covers:

- Training of administrators for all of the provisioning capabilities of the network including device management, Customer Relationship Management (CRM), and priority provisioning, profile definition and assignment.
- User account management.
- Resolving issues users may have with their devices, the network, and applications.
- Device administration in terms of maintaining inventories, asset tracking, and handling changes in assignments.
- Security administration for complying with the security policies and procedures, dealing with fraud in regard to any of the agency's devices or users, and any security related items in relation to the NPSBN.
- Change management for managing, scheduling and implementing changes to the network systems or processes.

### 4.7.2 Actors

- Agency User Administrator: deals with issues the end-users may have using their devices, applications, or the network as well as user account management changes such as an end-user's device or profile.
- Agency Device Administrator: has responsibility for interaction with local public safety users regarding any issues or account management administration.
- Agency Security Administrator: has responsibility for network security administration, which could include activities such as configuring security functions in the network and on the device, monitoring for network intrusion, and assuring the network meets the agency's local security standards.
- IT network administrator: responsible for setting up and maintaining a variety of general purpose (as opposed to LTE) network elements such as switches, routers, firewalls, printers, DNS servers, Mail Servers, databases servers. Depending on the organization, it may be very broad or very narrow, but is usually characterized as very general to the organization
- Responder: police, fire, emergency medical services, and secondary responders, etc.

### 4.7.3 Pre-conditions

1. It is assumed that the fully redundant transmission connection between the NPSBN Point of Presence (POP) and individual agency PSEN has been designed, tested, and established. In this case, the agency has chosen to host their own IT infrastructure and not outsource it to FirstNet.
2. Other aspects of the technical integration have been completed including:
  - a. Federating identities, integrating those identities with the local user stores, mobile Virtual Private Network (VPN), firewall changes, and a device management system
  - b. Integration of legacy and new databases and applications including access control and QoS, if necessary

- c. Systems or web access to systems, standard across all agencies, have also been provided to enable local control and have also been installed and tested and ready to use
  - d. Integration with existing agency systems and processes
  - e. All software has been upgraded with the necessary releases
3. It is also assumed that all the necessary agreements, policies, and procedures are in place such as a service level agreement (SLA) between FirstNet and the agency, security policies and procedures, common operating procedures, and industry best practices.

#### 4.7.4 Post-conditions

1. The user administrators are able to proficiently provide user account management services as well as resolve issues the end-users may have. They act as the helpdesk (tier 1) to provide assistance to first responders on how to operate their devices and accessories, applications and deal with any other usage issues they may have. They are familiar with the local control CRM and device management systems or web interfaces.
2. The dispatchers are able to proficiently use the new local control systems including device management, and priority provisioning.
3. The accounting administrators are proficient in generating and reading the accounting and billing reports.
4. The device administrators are proficient at resolving issues with end-users, ordering devices, accessories and Universal Integrated Circuit Card (UICCs), maintaining device, accessories and UICC inventories, loading a device with a UICC, handling device returns and repairs, and generating and reading the relevant reports.
5. The field operations are proficient with the systems, processes and procedures for submitting operational notifications for maintenance, performance, troubleshooting, and monitoring. They are also proficient with generating and reading for usage, outage, performance, restoration, throughput, and interference NPSBN reporting. Equally, they are able to provide the necessary network statistics reporting for the local Radio Access Network (RAN) to the NPSBN's Network Operations Center (NOC).
6. In-vehicle devices for the agency have been upgraded or replaced to support band 14.

#### 4.7.5 Frequency of Use

Many of the administrative procedures and processes will be followed on an on-going, daily basis. Training, though, will be refreshed at regular intervals and when there are major upgrades that change their processes and procedures of the administrative systems.

#### 4.7.6 Normal Course of Events

The following use cases are not exhaustive but provide an example for each area. During the Initial Operating Conditions (IOCs), all workflows will be developed.

##### 4.7.6.1 Training (End User Training, A.2.1.5)

1. A training methodology and materials have been developed to be provided to all agencies.
2. A time has been scheduled to do the training over a number of sessions with identified administrators of an agency. Not all administrators are required to attend all sessions.
3. The materials for each session contain presentation materials as well as hands-on exercises with the new systems (Training Users on Agency Specific Applications and Procedures, A.2.1.5.3).

4. To maintain concurrency with any changes, new training sessions will be held to cover the relevant topics either in person or on-line (Training on FirstNet Processes and Procedures, A.2.1.5.1).
5. Feedback from the training sessions will be used by the NPSBN operator to improve the ease-of-use and efficiency of the processes and procedures.

#### **4.7.6.2 User Administration (Agency User Subscription Management, A.2.1.3.3)**

The following use case describes the end-user having an issue with their device which turns out to be access permissions.

1. While out on duty the first responder, Ed, is unable to access a certain application. The first responder sends a message to the user administrator helpdesk (Customer Service Support, A.2.1.2).
2. The user administrator, Sharon, logs into the CRM system and reviews any recent issues or account management changes for Ed.
3. She notices that he recently changed departments with the consequence that Ed's access permissions may not have been updated by the agency's IT network administrator.
4. Sharon issues a ticket for the IT network administrator to check whether her assumption is correct.
5. The IT network administrator confirms the issue, updates Ed's permissions on the legacy application (Manage Authorization Services, A.7.1.4.4), and closes the ticket.
6. Sharon informs Ed that the issue has been fixed.

#### **4.7.6.3 Device Administration (Device Administration, A.2.1.3.1)**

Device administration deals with resolving device specific issues with end-users, ordering devices, accessories and UICCs, maintaining device, accessories and UICC inventories, loading a device with a UICC, handling device returns and repairs, and generating and reading the relevant reports.

The following use case describes an upgrade to an existing in-vehicle router to support band 14 (Installation of In-Vehicle Devices, A.2.1.3.2.4.1; Inventory/Service Fulfillment Management, A.2.1.3.2).

1. The device administrator, Joe, logs-in into the device inventory system and sees that some of the public safety vehicles are due to have their in-vehicle routers upgraded to support band 14.
2. Joe checks the inventory of the necessary upgrade parts, orders them (*Manage Device Ordering, A.2.1.3.2.2*), and gets them shipped to the local installation shop for their public safety vehicles (Device and Accessory Inventory Management, A.2.1.3.2.4).
3. Joe enters into the system that the parts are replacements for some older 3G modems cards for the routers as part of the purchase order to the installation shop.
4. Joe also calls up the local installation shop and confirms the appointments for the vehicle installations and to inform them that the modems have been ordered. The installation shop has been approved by the device Original Equipment Manufacturer (OEM) to work on their routers without voiding the guarantee.
5. After the vehicles have been upgraded, Joe provisions the in-vehicle routers appropriately (Provisioning of Users, A.2.1.3.3.1.3). The installation shop returns the old modems to the 3<sup>rd</sup> party handling returns.
6. Joe notes in the inventory system that the modems have been replaced and returned to the 3<sup>rd</sup> party handling returns (Manage Device Returns, A.2.1.3.2.1; Manage Stocking of Devices, A.2.1.3.2.3).

#### 4.7.6.4 Security administration

With each device, a pre-provisioned UICC card is provided. One duty of the security administrator, therefore, is to coordinate ordering a device as well as a UICC, inserting the correct UICC into the device for a user, and then registering the information in the International Mobile Equipment Identity (IMEI)/ UICC database. In some cases, the UICC may be embedded in the device and in that case, the security administrator's responsibility is only to provision the embedded UICC correctly.

1. The security administrator, Maria, logs-in into the device inventory system and orders a new device for a new recruit. She also checks that she has enough UICCs in stock locally at the agency.
2. On receiving the device, Maria, inserts a UICC into the device and provisions the UICC with the correct information for the new recruit including the credentials for the user (UICC Installation on Device, A.2.1.3.1.1.2). The officer may need to be present to complete the registration of the credential before the system can update the UICC, for example a derived Personal Identification Verification (PIV-I) credential.
3. Maria also updates a database that assigns the identifier of the UICC to that of a device, the IMEI (IMEI/UICC Inventory Management, A.2.1.3.1.1.1).
4. Maria notifies the user administrator that that the device and UICC are ready for when the new recruit arrives and that she can be on hand in case any help is needed.

#### 4.7.7 Alternative Courses

In areas of user and device administration, there will likely be many processes and procedures flows, some quite complex, that will need to be developed by the agencies and shared as best practices amongst agencies. Only simple examples of each are given here to illustrate the extent of the areas needed to be covered by agencies.

#### 4.7.8 Exceptions

None identified at this time.

#### 4.7.9 Includes

1. Local Control.1, Services, Applications, Users, and Device Management
  - a. Provisioning, de-provisioning of users (shared devices in this case).

#### 4.7.10 Special Requirements

None identified at this time.

#### 4.7.11 Assumptions

None identified at this time.

## 4.7.12 Operational Architecture Referenced Functions

Table 2 Customer Life Cycle.1 References to Operational Architecture

Operational Architecture Reference	Operational Architecture: Function Name
A.2	Life Cycle Management
A.2.1.1	User Security Administration
A.2.1.2	Customer Service Support
A.2.1.3.1	Device Administration
A.2.1.3.1.1.1	IMEI/UICC Inventory Management
A.2.1.3.1.1.2	UICC Installation on Device
A.2.1.3.1.3	Over The Air (OTA) Management
A.2.1.3.2	Inventory/Service Fulfillment Management
A.2.1.3.2.1	Manage Device Returns
A.2.1.3.2.2	Manage Device Ordering
A.2.1.3.2.3	Manage Stocking of Devices
A.2.1.3.2.4	Device and Accessory Inventory Management
A.2.1.3.2.4.1	Installation of In-Vehicle Devices
A.2.1.3.3	Agency User Subscription Management
A.2.1.3.3.1.2	De-Provisioning of Users
A.2.1.3.3.1.3	Provisioning of Users
A.2.1.5	End User Training
A.2.1.5.1	Training on FirstNet Processes and Procedures
A.2.1.5.3	Training Users on Agency Specific Applications and Procedures
A.7.1.4.4	Manage Authorization Services

## 4.8 Local Control.1: Services, Applications, User, and Device Management

This use case includes local administration to manage policies and provisioning for services, applications, users, and devices.

### 4.8.1 Description

This use case describes how a public safety entity (PSE) manages services, applications, users, groups, and devices via local control. One of the key components of FirstNet is to enable the control of these by local agencies. The capabilities addressed include:

- enabling the PSE to establish services, applications, user, group, and device policies specific to the PSE
- managing application, user, group, and device profiles
- provisioning new users, groups, and associated services
- changing and deleting users and groups

- managing devices
- dynamically assigning, enabling, and managing visiting PS users

#### 4.8.2 Actors

- PSE Chief of Administration
- PSE IT/Network Administrator
- PSE User Administrator
- PSE Device Management (DM) Administrator
- PSE New User
- PSE Existing User
- Communications Unit Leader (COML)
- Visiting Public Safety (PS) User
- FirstNet Local Control system
- FirstNet core network elements
- FirstNet Business/Operations Support Systems (B/OSS)

#### 4.8.3 Pre-conditions

1. Default QPP levels for services, applications, and users are set via FirstNet and NPSBN operator policies (QPP Administration A.7.1.6).
2. Local control is defined by the following table:

**Table 3 Local Control Definition**

Key Function	Local Control Function	Operational Architecture
<b>Account Management</b>	Manage PSE subscriptions, billing, purchasing, and accounts	A.4.4, A.8.6, A.3.5.2.6
	Manage and monitor PSE usage	A.3.5.2.1.1, A.3.5.4.4.2
	Manage PSE trouble tickets	A.2.1.2, A.3.8.3.1.2
	Training and certification for all users of local control capabilities, including PSE administrators, incident commanders, and COML	A.2.1.5
<b>Identity, Credential, and Access Management (ICAM)</b>	Identity management of PSE users	A.7.1.4, A.3.8.2.5.2
	Manage credentials of PSE users	A.7.1.4, A.3.8.2.5.2
	Management of user profiles including roles and attributes	A.2.1.3.3, A.4.3
	Manage access policies for users/groups, devices, services, and applications based upon roles and attributes	A.7.1.4
<b>User and Group Management</b>	Generic standard (NPSBN default) user profiles across various PSE agencies	A.4.1, A.4.3
	Manage user and group policies if different from NPSBN defaults	A.2.1.3.3, A.4.3, A.3.3, A.3.4.2.1, A.3.5.1, A.7.1.6.2
	Manage user/group subscriptions	A.2.1.3.3, A.4.3, A.3.4.2.1, A.3.5.1, A.9, A.9.2., A.9.3., A.9.4.
	User/group provisioning: new, activate, change,	A.2.1.3.3.1, A.3.4.2.1,

Key Function	Local Control Function	Operational Architecture
	deactivate	A.3.5.1, A.4.1, A.4.3, A.7.1.6.2
	Manage devices per user/group, including visiting users	A.2.1.3.3.1, A.3.4.2.1, A.3.5.1, A.4.3, A.7.1.6.2
	Manage services per user/group, including visiting users	A.2.1.3.3.1, A.3.4.2.1, A.3.5.1, A.4.3, A.7.1.6.2
	Manage DBs and resources per user/group, including visiting users	A.2.1.3.3.1, A.3.4.2.1, A.3.5.1, A.4.3, A.7.1.6.2
	Manage applications per user/group, including visiting users	A.2.1.3.3.1, A.3.4.2.1, A.3.5.1, A.4.3, A.7.1.6.2
	Dynamically manage user/group and QoS, Priority, and Preemption (QPP) profiles per user/group, including visiting users, based upon roles, attributes, and defined triggers. Examples of triggers can include user role changes per NIMS/ICS or local policies, responder emergency declared via “emergency button” on device, arrival of non-local visiting users providing mutual aid, or periods of local network congestion. The management interface may be delivered via a web, application, back-office system, or Computer-Aided Dispatch (CAD) interface.	A.4.3, A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.7.1.6.1
<b>Device Management</b>	Manage device policies if different from NPSBN defaults	A.2.1.3.1
	Manage device procurement, catalog, inventory, and profiles	A.2.1.3.2, A.8.7
	Configure devices and UICCs per PSE policies	A.2.1.3.1, A.2.1.3.1.3, A.3.8.2.3.4
	Device provisioning: new, activate, change, deactivate	A.4.1
	Manage embedded apps per device, per user	A.2.1.3.1, A.8.7.2
	Manage preloaded apps per device, per user	A.2.1.3.1
	Dynamically manage device and QPP profiles per device based on roles, attributes, and defined triggers	A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.7.1.6.1
	Mobile Device Management (MDM): Over The Air (OTA) device management, software installation, upgrades, configuration management, application management, remote trouble-shooting, lock and wipe, blacklist	A.2.1.3.1, A.2.1.3.1.3, A.2.1.3.1.4, A.3.4.2.2.7, A.3.8.2.3.4, A.7.1.9
<b>Services Management</b>	Manage services per user, per group, per device, per app	A.2.1.3.3.1, A.3.5.1, A.4.3, A.3.3
	Dynamically select QPP profiles for NPSBN network services based upon PSE policies and incident situations. It is expected the NPSBN will provide an array of pre-determined services profiles from which the PSE can select based on role, attributes, and defined triggers. However, it is not expected that the PSE will directly configure network services parameters or their profiles.	A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.7.1.6.1
<b>Applications Management</b>	Manage policies for local apps: applications provided by the local PSE for its users and approved visiting users	A.3.3, A.3.4.2.9.2, A.3.5.1, A.7.1.6.2

Key Function	Local Control Function	Operational Architecture
	Manage policies for local DBs and resources: resources available to local and approved visiting users such as video cameras, floor plans, motor vehicle information, and local incident reports	A.3.3, A.3.4.2.9.2, A.3.5.1, A.7.1.6.2
	Dynamically manage application and QPP profiles for local apps, DBs, and resources based on role, attributes, and defined triggers	A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.7.1.6.1
	Manage policies for FirstNet apps: applications provided by the NPSBN and available via the FirstNet app store, including FirstNet cloud services	A.3.3, A.3.5.1, A.3.4.2.7.2, A.7.1.1.1, A.7.1.6.2, A.7.2.3.5
	Manage policies for FirstNet interoperable DBs and resources: resources available to nationwide users through FirstNet such as FBI CJIS, NICS, NEMIS, and NFIRS	A.3.3, A.3.5.1, A.3.4.2.7.2, A.7.1.1.1, A.7.1.6.2, A.7.2.3.5
	Dynamically manage application and QPP profiles for FirstNet apps, DBs, and resources based on role, attributes, and defined triggers	A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.7.1.6.1
	Manage policies for third-party apps: applications provided by non-local, state, regional, tribal, or national PSEs. Expect local PSE to abide by policies of app owner.	A.3.3, A.3.5.1, A.3.4.2.9.2, A.7.1.6.2
	Manage policies for third-party DBs and resources: resources available at the discretion of other local, state, regional, tribal, or national PSEs. Expect local PSE to abide by policies of DB or resource owner.	A.3.3, A.3.5.1, A.3.4.2.9.2, A.7.1.6.2
	Dynamically manage application and QPP profiles for third-party apps, DB, and resources based on role, attributes, and defined triggers	A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.3.4.2.9.2, A.7.1.6.1
	Manage policies for commercial apps: applications provided by commercial app vendors, SaaS cloud providers, product vendors, or non-FirstNet app stores such as Google Play, Apple App Store, Windows Store, and BlackBerry World. Expect local PSE to abide by policies of app owner/vendor.	A.3.3, A.3.5.1, A.3.4.2.9.2, A.7.1.6.2
	Manage policies for commercial DBs and resources: resources available via commercial providers. Expect local PSE to abide by policies of DB or resource owner/vendor.	A.3.3, A.3.5.1, A.3.4.2.9.2, A.7.1.6.2
	Dynamically manage application and QPP profiles for commercial apps, DBs, and resources based on role, attributes, and defined triggers	A.3.3, A.3.5.1, A.3.4.2.1.2, A.3.4.2.7.3, A.3.4.2.9.2, A.7.1.6.1
	Apps provisioning: new, activate, change, deactivate	A.2.1.3.3.1.3.3, A.2.1.3.3.1.2.3, A.4.1
	Manage inter-agency agreements required for reciprocal use of apps, DBs, and resources	A.2.1.3, A.2.1.3.2
	Manage apps whitelists and blacklists per PSE, per user/group, per device	A.2.1.3.3.1.3.3, A.2.1.3.3.1.2.3, A.2.1.3.3, A.3.4.2.7.2, A.3.4.2.9.2, A.7.2.3.5
<b>Network Design</b>	NPSBN design consultation in areas such as cell site location, priority locations for coverage, backhaul	A.3.2, A.3.4.2

Key Function	Local Control Function	Operational Architecture
	design, network upgrades, network extensions, site hardening, and use of deployables	
	Consultation regarding incorporation of local network assets into network design such as reuse of LMR sites or backhaul such as dark fiber, microwave, or MPLS networks	A.3.2, A.3.4.2
	Consultation regarding locally funded site hardening, deployables, or network element deployment consistent with NPSBN policies	A.3.2, A.3.4.2
	Specification of access requirements from NPSBN to the local PSE network, IP space, services, applications, and resources. Interconnection may require a private access point name (APN) or VPN connection.	A.4.2, A.3.8.2.4.3.6
<b>Network Operations and Management</b>	Monitoring of network congestion status, fault status, planned/unplanned outages, local traffic volumes, SLAs, upcoming maintenance schedules, and security status	A.2.1.4, A.2.1.4.1, A.3.4.2.5, A.3.8.3.1, A.3.8.3.2, A.3.8.3.4
	Final authorization of planned maintenance outages to ensure there is not an unplanned incident during the planned outage	A.2.1.4, A.3.8.2.6
	Trouble-shooting and remediation of PSE security issues	A.3.8.3.2, A.3.8.3.4
	Update NPSBN network elements and back-end systems per the time of service delivery (latency) SLAs to reflect changes to accounts, ICAM, users, groups, devices, services, and applications made via local control	A.3.6.4
	Operation and management of locally funded or provided network assets, including deployables and local/state RANs, per agreement with the NPSBN operator	A.4.2, A.3.8.2.2, A.3.8.3.1
	Network reconfiguration, use of deployables, QPP changes, and operation during times of congestion or significant incidents requires a collaborative effort with FirstNet and the NPSBN operator	A.3.4.2.1.2.2, A.3.8.2.6, A.3.8.3.1

The following are excluded from local control.

- PSEs do not have local control over the following, which are administered by the NPSBN operator:
  - a. QPP level of basic network services. FirstNet and the NPSBN operator will use standards-driven QPP profiles for basic network services such as IMS control signaling, conversational voice, guaranteed bit rate (GBR) data, and non-GBR data. This is meant to optimize PS operations 1) to provide a best practices approach to basic wireless network service delivery and 2) to ensure that applications and users mapped to services receive the same minimum level of QoS in multi-vendor network deployments and in cases of roaming. FirstNet is open to discussions with a state or regional PS

- authority on the configuration of basic network services for their jurisdiction and crafting updates if there are local conditions that require changes to basic network services profiles.
- b. Access Class in UICC.
  - c. Public Land Mobile Network (PLMNs) and roaming agreements.
3. The PSE has an enterprise administrative account with the NPSBN operator that includes access to a portal or other interface that enables local control. The interface is branded with the logo of the PSE along with color scheme and other configuration options controlled by the PSE (Local Control User Administration Arch, A.3.4.2.1).
  4. The PSE IT/network administrator, PSE user administrator, PSE DM administrator, and COML have completed training and are certified in the use of the NPSBN local control system (User Training, A.2.1.5). Each has established credentials for accessing the system and is enabled when the local agency is on-boarded with FirstNet (Identity Management, A.7.1.4).
  5. PSE users have completed training for use of FirstNet devices, services, and applications (User Training, A.2.1.5).
  6. Training, job aids, and best practices for utilizing the local control system are provided by the NPSBN operator, to assist with the PSE's service order governance (Define, Monitor, and Implement Provisioning Policies and Procedures A.4.1, Develop Best Practices A.4.5).
  7. The PSE IT/network, user, and DM administrators operate out of a PSE office and utilize commercial laptops running commercially available operating systems.
  8. The COML operates in the field and utilizes Band 14-capable devices such as a smartphone or tablet.
  9. SLAs are in-place between FirstNet and the NPSBN operator re: the latency between when the PSE administrators and COML make changes via their local control interfaces and when those changes are operational within the NPSBN. See use case Operations.4, Network Management
  10. The PSE's local control capabilities are not dependent upon whether the state is opt-in or opt-out (User Migration for Opt-Out States, A.9.1).
  11. All PSE end-users have had their identities proofed, with PSE-specific credentials established. See use case Applications.1, Identity, Credential, and Access Management (ICAM)
  12. Local control system is tested and verified to meet FirstNet acceptance per test strategy documentation. (Quality Assurance and Testing A.3.8.2.4, Configuration Testing A.3.8.2.4.5)
  13. Local control system meets FirstNet's requirements for hardening, resiliency, redundancy, and security. (Quality Assurance and Testing A.3.8.2.4, Configuration Testing A.3.8.2.4.5, System Hardening Design A.3.4.2.8, Reliability Design A.3.4.2.8.1, Resiliency Design A.3.4.2.8.2, Security Systems Management A.3.8.2.5, User Security Administration A.2.1.1)
  14. Local control system works in conjunction with FirstNet and contractor's B/OSS systems to provide the following (Billing Systems Maintenance A.3.5.4).
    - a) Allow for local control updates and transactions to be billed or not billed depending on the type of update and who initiates the change.
    - b) Allow FirstNet to charge its end users for local control as a service:
      - i. Utilizing a flat rate billing model for so many updates per period with estimated charges for additional updates
      - ii. Utilizing a per update billing model

- iii. Allowing agencies, FirstNet end users, to pool resources and needs for local control usage and billing.

#### 4.8.4 Post-conditions

1. The PSE entity follows applicable FirstNet and NPSBN operator governance and guidelines in the creation and management of QPP policies for their agency (Define Standard Policies for User Profiles, A.4.3).
2. New users are provisioned on the NPSBN, with a user profile that identifies the services and applications which they are allowed to access. That profile is specific for this particular public safety enterprise network (PSEN) and its users (Define Standard Policies for User Profiles, A.4.3).
3. In-service devices are assigned to users. A user may be assigned multiple devices. See use cases See use case Devices.1, Device Ecosystem; Devices.2, Mobile Device Management (MDM); Devices.3, Bring Your Own Device (BYOD)
4. Policy, application, user, and device provisioning changes have propagated from the local control system to the appropriate NPSBN network elements and back-office systems (KPI monitoring A.3.6.4).
5. Visiting non-local PS users providing mutual aid are successfully added to the local resources assigned to an incident under command of the local PSE and removed after the incident is complete (Local Control User Provisioning and Administration A.2.1.3.3.1, Local Control User Administration Architecture .3.4.2.1, Local Control: Service and User Provisioning A.3.5.1, Define Standard Policies for User Profiles A.4.3, Management and Enablement of Static User Profiles A.7.1.6.2).

#### 4.8.5 Frequency of Use

This situation occurs continuously on a nationwide basis.

#### 4.8.6 Normal Course of Events

For the following scenarios, except where noted, all references to the Operational Architecture are included in the local control definition presented previously (see Section 4.7.12, Operational Architecture Referenced Functions).

##### 4.8.6.1 Services and Applications Policy Management

1. PSE Chief of Administration works with PSE leadership to set agency policies regarding:
  - a. Services to be provided to PSE users
  - b. Applications allowed for use by PSE users. Applications include those available via local, FirstNet, third-party, or commercial app stores
  - c. QPP rules of the local applications owned and provided by the PSE
  - d. QPP rules of the FirstNet applications used by the PSE if different than the default QPP
  - e. The list of PSE applications used when a responder emergency condition has been initiated. This list of applications is given the highest NPSBN priority and may preempt, if necessary other resources and applications
  - f. Whether or not applications identified during immediate peril conditions may preempt, if necessary, other resources and applications
  - g. Applications whitelists and blacklists based upon devices, users, and roles

- h. Retention, archival, and back-up policies for application profiles
    - i. Auditing and governance of the PSE policy rules with those of FirstNet and the NPSBN operator.
2. The PSE IT/network administrator logs into the NPSBN local control system and enters a new service order request. A unique service order code is created, time-stamped, and logged. This allows for tracking of all orders managed through the NPSBN local control system.
3. The PSE IT/network administrator updates the agency policies in the NPSBN local control system per the policies provided by the PSE Chief of Administration. The system performs a preliminary validation of any data input to check the data is consistent with policy rules before further processing of the requested updates.
4. Within the established SLAs, the new policies are provisioned into the appropriate network elements and back-office systems of the NPSBN operator.
5. The order is closed in the NPSBN local control system.
6. Authorized users of the local control system, such as the PSE Chief of Administration and PSE administrators, are able to generate reports and analytics on the service orders processed through the NPSBN. Reporting must also be available to FirstNet and NPSBN operator administrators.
7. All the service order history and logs are stored for the period of time as set by policy, to satisfy auditing and compliance requirements for both FirstNet and the PSE.

#### **4.8.6.2 Application Management**

1. The PSE IT/network administrator leverages the NPSBN local control system to manage all aspects of the agency's applications lifecycle. The applications management steps taken by the administrator include the following.
  - a. Manage application profiles, including versions, QPP, platform requirements, device compatibility, supplier, and support contacts
  - b. Manage the activation and deactivation of applications, including updates to the agency's applications whitelist and blacklist
  - c. Manage purchasing and the ongoing application billing accounts from local, FirstNet, third-party, and commercial app stores. See use case Applications, App Stores: FirstNet, Local, Commercial
  - d. Manage inter-agency agreements required for reciprocal use of database resources and applications
  - e. Manage the embedded, and any pre-loaded mobile device applications in collaboration with the PSE DM administrator
  - f. Manage application performance monitoring and trouble-ticket escalation with suppliers

#### **4.8.6.3 User and Group Policy Management**

1. PSE Chief of Administration works with PSE leadership to set agency policies regarding:
  - a. Supported and non-supported PSE user and group roles. Identify roles such as law enforcement officer, incident commander, fire fighter, and emergency medical technician (EMT) that are recognized by FirstNet.

- b. Key user and group attributes that are required in each user and group profile. Examples of attributes can include training certifications, security clearance, language skills, different skillsets, and others.
  - c. User and group access to services, applications, and devices based upon their role and attributes.
  - d. Access to resources such as restricted databases provided to users and groups based upon their role and attributes. The PSE must take into account the governance policies related to national database access such as security, PSE VPN, and user credentials.
  - e. Identification of which users may initiate and clear responder emergency, immediate peril, and incident state conditions.
  - f. QPP rules for the roles supported by the PSE.
  - g. QPP rules based on the attributes of PSE users and groups.
  - h. Retention, archival, and back-up policies for user and group profiles.
  - i. Auditing and governance of the PSE policy rules with those of FirstNet and the NPSBN operator.
2. The PSE user administrator logs into the NPSBN local control system and enters a new service order request.
  3. The PSE user administrator updates the agency policies in the local control system per the policies provided by the PSE Chief of Administration.
  4. The order is closed in the local control system.

#### 4.8.6.4 New User Provisioning

1. A PSE user administrator receives a request to set-up, configure, and provision a PSE new user.
2. The PSE user administrator logs into the NPSBN local control system and enters a new service order request.
3. The PSE user administrator creates a new user profile per basic templates defined by FirstNet and the NPSBN operator. The profile contains key information about the new user such as name, agency, default role, and key attributes that are captured per PSE policy.
4. Based upon the user profile, the new user is subscribed to a specific set of services and applications. In addition, the user profile is used to set the new user's QPP levels per PSE policy.
5. The new user is added to the account of the PSE, with charging and billing rules per the PSE's account with the NPSBN operator. The PSE has a rate plan which has been subscribed from the NPSBN operator.
6. The new user is assigned one or more PSE devices per user and DM policies.
7. The new user profile is linked to the user's identity profile and credential database maintained by the PSE. See use case Applications.1, Identity, Credential, and Access Management (ICAM).
8. Within the established SLAs, the new user is provisioned into the appropriate network elements of the NPSBN and is activated in the charging, billing, and customer care systems of the operator.
9. The order is closed in the local control system.
10. A PSE user administrator receives a request to set-up, configure, and provision a large number of new users. The bulk profile data for the users is available in a format that can be uploaded to the local control system.

11. The PSE user administrator logs into the NPSBN local control system and enters a new order request.
12. The PSE user administrator uploads the bulk user information and manages the order to create and provision all the new users, closing the service order when complete.
13. If there is any issue on access or provisioning of the users, customer care and support are available from the NPSBN operator for technical and administrative issues at various levels.

#### 4.8.6.5 Changing or Deleting Users

1. A PSE user administrator receives requests to make a change to a PSE existing user to reflect his or her new role in the PSE, and to delete another user due to termination from the PSE.
2. The PSE user administrator enters a new service order request into the NPSBN local control system for the user role change.
3. The PSE user administrator changes the existing user profile. All changes that result from the new role to services, applications, and QPP are made by the local control system without manual intervention by the administrator.
4. Per SLAs, the change is reflected in the network elements and back-office systems of the operator.
5. The order is closed in the local control system.
6. The PSE user administrator enters a new service order request for deleting a user.
7. The PSE user administrator marks the user profile to deactivate access to the network, services, and applications.
8. The user is deactivated against the PSE's account for charging and billing purposes.
9. All devices assigned to the deactivated user are flagged for deactivation and retrieval.
10. Per SLAs, the deactivation is reflected in the network elements and back-office systems of the operator.
11. The order is closed in the local control system.
12. Archival and eventual deletion of the user profile is governed by PSE policy.

#### 4.8.6.6 Device Policy Management

1. PSE Chief of Administration works with PSE leadership to set agency policies regarding:
  - a. The approved list of FirstNet certified devices provided by the PSE that includes a wide variety of Band 14-capable device types including smartphones, In-Vehicle Routers (IVR), laptops, cameras, and sensors. See use case Devices.1, Device Ecosystem.
  - b. Identification of which users and/or roles can access which devices.
  - c. The support, or not, of Bring Your Own Devices (BYOD) by the PSE. See use case Devices.3, Bring Your Own Device (BYOD).
  - d. The approved list of devices the PSE will accept for BYOD.
  - e. Identification of which users and/or roles can BYOD.
  - f. Applications to be preloaded on which devices.
  - g. Applications to be preloaded based upon assigned users and their roles.
  - h. Retention, archival, and back-up policies for device profiles.

2. The PSE DM administrator logs into the NPSBN local control system and enters a new service order request.
3. The PSE DM administrator updates the agency policies in the local control system per the policies provided by the PSE Chief of Administration.
4. The order is closed in the local control system.

#### **4.8.6.7 Mobile Device Management**

The PSE DM administrator needs to manage all aspects of the agency's device lifecycle, including the ability to manage a device catalog, device inventory, activations, software/firmware management, content management, UICC registration, embedded applications, pre-loaded applications, device deactivations, and transfers. See the following use cases: Devices.1, Device Ecosystem, Devices.2, Mobile Device Management, Devices.3, Bring Your Own Device (BYOD)

#### **4.8.6.8 Multi-Jurisdictional Incident Response Management**

1. FEMA has defined five (5) types of incidents (FEMA Types 1-5) based upon the level of complexity and required resources. See the following use case Incidents.5, FEMA Type 5: Traffic Stop for an example of local control in a Type 5 incident.
2. See the following use case Incidents.4, FEMA Type 4: Terrorist Surveillance for an example of local control in a Type 4 incident that involves dynamically assigning, enabling, and managing visiting PS users.
3. Type 1-3 incidents involve an Incident Command Structure (ICS) to provide leadership and coordination across multi-jurisdictions that may involve local, state, regional, tribal, and federal PSEs. In these types of incidents, the role of the Communications Unit Leader (COML) is expected to provide the local control for managing communications groups, services, and applications. See the following use case QPP.1, Quality of Service, Priority, and Preemption (QPP) for an example of local control in a Type 3 incident that involves dynamically assigning, enabling, and managing visiting PS users.

#### **4.8.7 Alternative Courses**

Local Control.1.AC.1. PSE changes its services subscription with the NPSBN operator to add a high-quality video service

1. Insert at Sec 1.8.1 Step 1 in Normal Flow.
  - a. Assess and update PSE services and applications policies as needed, in particular supported services, applications, responder emergency, immediate peril, and whitelist/blacklists.
2. Insert at Sec 1.8.2 Step 1 in Normal Flow.
  - a. Assess and update PSE applications profiles as needed, in particular supported applications, purchasing, and pre-loaded list of applications.
3. Insert at Sec 1.8.3 Step 1 in Normal Flow.
  - a. Assess and update PSE user policies as needed, in particular allowed services, applications, and devices based upon role.
4. Insert at Sec 1.8.5 Step 1 in Normal Flow.
  - a. Create form for bulk provisioning changes to add new service and applications to PSE existing users. Input form and complete provisioning changes as needed.

5. Insert at Sec 1.8.6 Step 1 in Normal Flow.
  - a. Assess and update PSE device policies as needed, in particular supported applications and pre-loaded list of applications.
6. Insert at Sec 1.8.7 Step 1 in Normal Flow.
  - a. Create form for bulk device provisioning changes to add new service and applications to devices of PSE existing users. Input form and complete provisioning changes as needed.

#### 4.8.8 Exceptions

Local Control.1.EX.1. Local PSE administrators lose access to NPSBN local control system, such that there is no ability to make policy, application, user, or device updates.

1. Create forms as needed to facilitate bulk changes.
2. Input forms and complete changes when system once again available to PSE administrators.

#### 4.8.9 Includes

1. Applications.1, Identity, Credential, and Access Management (ICAM)
  - a. Identity proofing, credentialing
2. Applications.3, App Stores: FirstNet, Local, Commercial
3. Devices.1, Device Ecosystem
  - a. Issuing, purchasing, replacing an existing device
  - b. Pre-loading applications
4. Devices.2, Mobile Device Management (MDM)
  - a. Troubleshooting, reset, wipe, polling, campaigns, device blacklisting
  - b. Local Control: activate, deactivate, lock, wipe
5. Devices.3, Bring Your Own Device (BYOD)
  - a. User opt-in
6. Operations.4, Network Management
  - a. Monitoring of performance against SLAs
7. Incidents.4, FEMA Type 4: Terrorist Surveillance
8. Incidents.5, FEMA Type 5: Traffic Stop
9. QPP.1, Quality of Service, Priority, and Preemption (QPP)

#### 4.8.10 Special Requirements

1. The local control solution must scale incrementally and cost-effectively to support up to 60,000 PSEs.
2. Service Level Agreements (SLA):
  - a. Latency from time updates made locally to realization in the NPSBN and the operator's back-office systems. See Quality Assurance Surveillance Plan (QASP) measures Q-APP-21 and Q-APP-22.

#### 4.8.11 Assumptions

1. QoS parameters typically apply to services and applications. However, QoS parameters can apply to users as well in the PS situations of responder emergency and immediate peril.
2. QoS, QPP parameters apply to services, applications, and users.
3. PSEs align to the structure and roles identified in the Department of Homeland Security (DHS) National Incident Management System (NIMS) and the Incident Command Structure (ICS).

#### 4.8.12 Operational Architecture Referenced Functions

The following provides a cross-reference between this use case and the functions in the operational architecture that are illustrated.

**Table 4 Local Control.1 Operational Architecture References**

Operational Architecture Reference	Operational Architecture Function Name
A.2.1.1	User Security Administration
A.2.1.2	Customer Service
A.2.1.3	Public Safety Entity Management
A.2.1.3.1	Device Administration
A.2.1.3.1.3	Over The Air (OTA) Management
A.2.1.3.1.4	Diagnostics Monitoring and Management
A.2.1.3.2	Inventory/Service Fulfillment Management
A.2.1.3.3	Subscription Management
A.2.1.3.3.1	Local Control User Provisioning and Administration
A.2.1.3.3.1.2.3	Services and Applications Deactivation
A.2.1.3.3.1.3.3	Installation of Services and Applications
A.2.1.4	Agency/State Network Monitoring
A.2.1.4.1	View Only of Network Status
A.2.1.5	User Training
A.3.2	Network Deployment
A.3.3	Priority and QoS Administration
A.3.4.2	Network Design and Architecture
A.3.4.2.1	Local Control User Administration Architecture
A.3.4.2.1.2	Development of Local Control User Operations Guideline
A.3.4.2.1.2.2	NIMS ICS Management
A.3.4.2.2.7	Device Management Planning and Design
A.3.4.2.5	Traffic Management
A.3.4.2.7.2	App Store Management
A.3.4.2.7.3	Service Delivery Platform Development
A.3.4.2.8	System Hardening Design
A.3.4.2.8.1	Reliability Design
A.3.4.2.8.2	Resiliency Design
A.3.4.2.9.2	3rd Party Applications Administration
A.3.5.1	Local Control: Service and User Provisioning
A.3.5.2.1.1	Usage Reporting to Users
A.3.5.2.6	Invoicing
A.3.5.4	Billing Systems Maintenance

Operational Architecture Reference	Operational Architecture Function Name
A.3.5.4.4.2	Usage Reporting to Users
A.3.6.4	KPI Monitoring
A.3.8.2.2	Network Change Management
A.3.8.2.3.4	Device Management Operations
A.3.8.2.4	Quality Assurance and Testing
A.3.8.2.4.5	Configuration Testing
A.3.8.2.4.3.6	PSEN Interconnection Testing
A.3.8.2.5	Security Systems Management
A.3.8.2.5.2	Personnel Identity Management
A.3.8.2.6	Disaster Response and Recovery (NIMS Types 1,2,3) and Major Planned Events
A.3.8.3.1	National Network Operations Center
A.3.8.3.1.2	Network Events
A.3.8.3.2	Agency Security Operations Center
A.3.8.3.4	Security Operations Center
A.4.1	Define, Monitor, and Implement Provisioning Policies and Procedures
A.4.2	Network Policies and Procedures
A.4.3	Define Standard Policies for User Profiles
A.4.4	Define, Monitor, and Implement Billing Policies and Procedures
A.4.5	Develop Best Practices
A.7.1.1.1	Application Publishing
A.7.1.4	Identity Management
A.7.1.6	QPP Administration
A.7.1.6.1	Management and Enablement of Dynamic User Profiles
A.7.1.6.2	Management and Enablement of Static User Profiles
A.7.1.9	Mobile Device Management Services
A.7.2.3.5	Cloud Services/Hosted Applications
A.8.6	User Fee Administration
A.8.7	Definition of Device Portfolio
A.8.7.2	Embedded Apps
A.9	User Migration and Evolution
A.9.1	User Migration for Opt-Out States
A.9.2	User Migration From Existing PS Private Wireless
A.9.3	User Migration From LMR Systems
A.9.4	User Migration From Commercial Networks

## 4.9 Local Control.2: Network Operations and Maintenance

This use case includes local administration to manipulate the network for the local agency's specific needs, including deployables.

### 4.10 QPP.1: Quality of Service, Priority, and Preemption (QPP)

This use case includes interface to applications with QoS requirements, dynamic priority, preemption, and control of secondary users.

### 4.10.1 Description

There is a large explosion at a chemical plant. A potential exists for hazardous chemical leaks as well as the release of toxic smoke from the burning chemicals. This use case focuses on the dynamic QPP aspects that come into play in this incident. It incorporates best practices, ideas, and requests regarding QPP from states and first responders.

### 4.10.2 Actors

- Law enforcement using 10 (and then 20) Push-To-Talk (PTT) priority Band 14-capable devices/users provisioned in a talk group, 5 high bit rate Machine-To-Machine (M2M) High Definition (HD) camera devices, and 5 M2M non-Guaranteed Bit Rate (GBR) Internet/database access devices
- Emergency Management using 10 (and then 20) PTT priority Band 14-capable devices/users provisioned in a talk group, 5 high bit rate M2M HD camera devices, and 5 M2M non-GBR internet/database access devices
- Fire service using 10 (and then 20) PTT priority devices/users provisioned in a talk group, 5 high bit rate M2M HD camera devices, and 5 M2M non-GBR internet/database access devices
- Local Incident Commander (IC)
- On-site mobile command center dispatch operator
- Regional command center “uber” dispatch operator
- Emergency Manager (EM) at the Emergency Operations Center (EOC)
- Secondary users and security guards at shopping area
- Hazmat teams

### 4.10.3 Pre-Conditions

1. IR.92 VoLTE used for incident voice communications (Voice Services A.7.2.5).
2. 3GPP IMS-based Push-To-Talk (PTT) is used for group communications (Mission Critical PTT Voice (3GPP) A.7.2.1).
3. Messaging via IMS IP messaging with capable handsets and network (Instant Messaging/SMS/MMS A.7.2.3.3.2-3).
4. Location services including z-direction determination is available on handsets and in the network.
5. Applications used include geo fencing, chemical analysis, FirstNet Operations and Maintenance (O and M) interface applications, Uber user FirstNet dispatcher software, databases, type of fires database (what is burning), and a building database regarding what flammable materials are on what floor.
6. When a user goes into parking garage requiring more power from eNB, other users are moved to non-GBR for non-priority services.
7. All dispatchers are FirstNet trained dispatchers and understand how to allocate network resources.
8. All dispatchers interface with FirstNet designed software which estimates eNB site and/or area capacity based on requested applications and services.
9. The devices all have a built-in GPS function, support location reporting, and are actively running the map display application. FirstNet’s network has location support including “z” direction support.
10. The Band 14 devices and associated PS applications are available and working for the first responders at the time of incident. The NPSBN is available for public safety responders.

11. All first responders' basic identities have been validated locally and authenticated.

#### 4.10.4 Post-conditions

1. Seamless hand-off between multiple cell sites as actors move.
2. Application continuity as the actors separate and cross cell boundaries.
3. Throughout the scenario, all communications and data are securely (encrypted) transmitted to the first responders via their LTE devices and to the incident command center.
4. Agency incident record that includes time-stamped location data, vehicle tracking, group messaging, and video records logged that enables post-action analysis and use as evidence.
5. Network and application usage records created for billing.
6. Any network logging or IMSI based tracking at application level logging, is captured for NPSBN operator analysis.

#### 4.10.5 Frequency of Use

This situation occurs daily on a nationwide basis.

#### 4.10.6 Normal Course of Events

1. A large explosion occurs at a chemical plant in Barberville, a suburb of Brookside. A potential exists for hazardous chemical leaks as well as toxic smoke emissions from the burning chemicals. A shopping area is near the chemical plant and one FirstNet eNB serves both the area around the chemical plant and the shopping area.
2. IC arrives on scene and assesses the situation. After briefly surveying the area, the IC team initiates its mobile command center, assumes QPP/local control, and begins to receive information from the on-site first responder vehicles and personnel.
  - a. Local IC requests and is granted (from jurisdictional regional command) operational local control and QPP for the five square mile area surrounding the chemical plant (QPP Administration A.7.1.6, Dynamic Incident Management A.7.1.6.1, Incident Command System (ICS) Service A.7.1.6.1.5, Real time Priority and Role Based Execution A.7.1.6.1.5.1., Immediate location and Priority Management A.7.1.6.1.6.1).
  - b. Jurisdictional regional command via "uber" FirstNet trained dispatcher and a geo-fence application overlaid with FirstNet eNB coverage area, creates geo-fence around chemical plant area and transfers operational QPP/local control to mobile command center including secondary user preemption command and control (Local Control User Administration A.2.1.3.3.1).
  - c. Now in control, the local on-site dispatcher (associated with IC) and geo-fence software have determined that the chemical plant area is served by only one FirstNet eNB (worst case scenario) (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1).
  - d. Based on the incident assessment (size and type), personnel, types of devices and applications are identified for three teams: an Emergency Management team (10 users and 10 devices), a Law Enforcement team (10 users and 10 devices) and a Fire team (10 users and 10 devices) (Group Communication (GCSE 3GPP) A.7.1.5).
  - e. IC assigns devices to the personnel in the identity management server and site teams' devices profile/priority classes are raised by the on-site dispatcher. The standard elevated profiles for this type of incident are invoked for each participating group personnel (and via the identity

- server to the devices assigned each user). The local agency provides access to the QPP profile to the IC and associated IMSI and user's profile. This access includes any non-local agency (mutual aid) first responder in that area able to get authenticated and authorized for all associated applications (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1).
- f. Emergency Management's elevated profile contains 10 PTT priority devices/users provisioned in a talk group, 5 high bit rate Guaranteed Bit Rate (GBR) HD camera devices, and 5 non-GBR internet/database access devices (chemical measurement wireless devices). The FirstNet network should be able to federate the identity if any non-local agency user wants to access external DB directly under the direction of IC (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communications (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Mobile Video Feeds A.7.2.3.1.1).
  - g. Law enforcement's elevated profile contains 10 PTT priority devices/users provisioned in a talk group, 5 high bit rate GBR HD camera devices, and 5 non-GBR internet/database access devices (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communications (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Mobile Video Feeds A.7.2.3.1.1).
  - h. Fire service's elevated profile contains 10 PTT priority devices/users provisioned in a talk group, 5 high bit rate GBR HD camera devices, and 5 Machine To Machine (M2M) non-GBR internet/database access devices (fire cameras and sensors) (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communications (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Mobile Video Feeds A.7.2.3.1.1).
  - i. After assigning the three teams' device quantities, their capabilities and application requirements based on a template (bit rate required, GBR, NGBR, latency), the on-site dispatcher via the dispatcher software has estimated that at full utilization these three groups will occupy 80% of the serving LTE eNB channel's capacity (without taking secondary traffic into account). The eNodeB associated for this event shall be able to provide the number of bearer resources available for first responders. Network operations logging is needed so there is no resource issue (Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2, Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1).
  - j. The dispatcher software, via hooks into FirstNet's operations network, checks the current traffic load on the incident area serving eNB and determines it is currently at 40% capacity from secondary and non-incident traffic (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2).
  - k. Therefore, the on-site dispatcher, via suggestions from the dispatch software application, instructs the eNB serving secondary user traffic to begin redirect of secondary and non-incident

user access attempts to other eNBs serving secondary users via access class barring. There is no need for preemption at this point. Security guards in the shopping area have access classes reserved for public safety and can continue to access FirstNet's LTE network as necessary. As eNB traffic load is shed, the dispatcher software instructs the eNB to limit secondary usage to 10% of capacity leaving 10% of eNB capacity margin (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2, Access Class Barring A.7.1.6.1.1).

- l. IC via the dispatcher software and on-site dispatcher sends an email or other agreed communication message to the operator leasing secondary capacity regarding the invocation of priority due to an incident, the location of the incident and a forecast of first responder priority status incident duration (Email A.7.2.3.3.1).
- m. All information is shared real-time with the Emergency Operations Center.

3. The Emergency Manager (EM) is alerted that a major incident has occurred and brings up the command terminal in the Emergency Operations Center (EOC) to monitor the regional situation. All of the region's assets are available for query by the EM.

4. The mobile command center's display registers all of the assets that are currently on scene, including emergency management, law enforcement (LE), and fire service. The status of each asset is also available, but is displayed on demand.

- a. Responders either enter the area with their devices, power them on, and confirm they are working correctly, or arrive at the mobile command center and are assigned the required devices. After connecting to the network, each device reports its position and status (Location Services A.7.1.10).
- b. As responders move from outside to inside the incident geo-fenced area their assigned devices show a priority flag indicating they are now assigned a higher priority class. If they leave the geo-fenced area, leave FirstNet coverage within the geo-fenced area, or roam to commercial LTE coverage, their priority flag will disappear, and alert them they no longer have priority network access (Data Services A.7.2.3).
- c. Active/attached devices report their status, assignment, and location every 60 seconds or as requested (Location Services A.7.1.10).
- d. Higher priority users with their situational awareness application should periodically report network connectivity, resiliency, and latency to the NOC (Homepage Situational Awareness A.7.2.3.5.3.1).

5. IC shifts the display to a GIS overlay of the explosion, with the location of all assets shown. Areas are marked to display casualties, fires, evidence, and the incident perimeter. The information for the GIS displays comes from a site survey already underway by law enforcement, fire, and emergency management personnel.

- a. IC downloads chemical plant building data including floor heights and assets on each floor to determine dangerous and safe areas. The third party provider application which has the floor plan of the plant is available to the IC and all to the high priority users. All cameras in the building plant, secondary user related to the utility, are accessed by the IC along with the ability to control it (Data services A.7.2.3, M2M Feeds A.7.2.3.4).
- b. IC requests z direction location for those responders traveling indoors. The GIS software gives IC a picture of where responders are within the building (x and y location) and on what floor (z axis) (Location Services A.7.1.10).

- c. IC communicates dangerous areas to responders and responders identify casualties by location. EM also has real-time access to this data (Location Services A.7.1.10).
6. Information is available on the EM's system as the information is gathered by IC. This information is shown both in a GIS map format as well as a textual set of data. On demand, the EM can call up the information on the incident as though the EM were on site in the capacity of IC.
  - a. Displays are mirrored at IC and EM screens.
7. As new units arrive on scene, they are authenticated into the incident and added to the list of assets available to IC (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1).
8. The on-scene fire branch monitors the status, location, and current duties of the fire assets on its command screen, and reassigns those assets as necessary. Any data that is pertinent to the other branches and IC is automatically forwarded to their command systems. This same situation is repeated for the LE branch as well as the emergency medical services branch.
  - a. HD cameras are activated and can be downgraded (as a first step) to non-GBR if eNB capacity reaches 90%. M2M HD cameras are capable of changing their refresh rate, encoding and modulation based on their GBR status and are notified via M2M message of their new bit rate status (GBR or non-GBR) so they can accommodate the new GBR priority class (M2M Feeds A.7.2.3.4, Mobile Video Feeds A.7.2.3.1.1).
9. After completing all of the pre-defined tasks for this particular type of incident, IC begins coordinating with the law enforcement, emergency medical services, and fire command posts. As IC begins directing the assets in the field, the fire branch informs IC that the incident is too large to be handled by the assets on hand.

IC then puts in a request to the EM for the acquisition of more fire units.

  - a. Fire service's assets are upgraded to 20 from 10. Fire's elevated profile now contains 20 PTT priority devices/users provisioned in a talk group (10 are added), the same 5 high bit HD camera devices, and 5 M2M non-GBR internet/database access devices (fire cameras and sensors) (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communication (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4).
  - b. After adding new users/devices to the talk group, dispatch software recommends to on-site dispatcher to change all GBR cameras to "best effort" non-GBR to accommodate additional users. M2M HD cameras are capable of changing their refresh rate, encoding and modulation based on their GBR status and are notified via M2M message of their new bit rate status (non-GBR, in this case) so they can accommodate the new GBR priority class. With cameras now at non-GBR, the new maximum load on the cell is 70% (Dynamic Incident Management A.7.1.6.1, QCI Management A.7.1.6.1.2, M2M Feeds A.7.2.3.4).
10. As the request for more fire assets comes into the EM, the EM initiates the mutual-aid agreements in place, and units are dispatched from the Brookside metropolitan area to Barberville.

11. The emergency medical services branch sets up a triage/treatment area, and begins to direct the resources available to identify and handle casualties. The location of the triage/treatment area is disseminated to all first responders on scene, and its status is made aware to area medical facilities.
  - a. SMS messages are sent periodically to all groups with information. The information should be encrypted between the devices to the emergency medical services application servers (Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3).
  
12. The fire branch is notified of an emergency on its command screen as one of the firefighters in the field has a wireless M2M sensor triggered by the detection of a hazardous chemical. The M2M sensor determines that the hazardous chemical would not be ignited by a radio transmission, allowing the network to notify all first responders within 100 feet of that particular firefighter along with law enforcement, emergency medical services, and IC. The fire branch designates this area as a hot zone, which alerts any personnel entering the designated area to its status.
  - a. IC creates a geo-fence 100 feet around the firefighter's location, designates it a "hot zone" and creates a temporary group. As users enter and/or leave the geo-fenced area, they are automatically added or deleted from this "hot zone" group. A message is triggered as a user enters or leaves the "hot zone" group (as the user is added/deleted from the group) (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communications (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3).
  - b. IC sends periodic SMS messages to active members of the "hot zone" group (Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3).
  
13. Because of the potential for the release of hazardous chemicals, the EM directs all available hazardous materials (hazmat) teams to the location and puts these assets under the control of IC.
  - a. To accommodate the new hazmat personnel, 10 additional users are provisioned into the EM group. Emergency management's elevated profile now contains 20 PTT priority devices/users provisioned in a talk group, 5 high bit rate GBR HD camera devices, and 5 non-GBR internet/database access devices (chemical measurement wireless devices) (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communications (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3, Mobile Video Feeds A.7.2.3.1.1).
  - b. The on-site dispatcher using the dispatch software application now determines the additional users cause the serving eNB load to increase to 90% (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2).
  - c. The dispatch software application suggests that the lowest priority public safety users, and the security guards in the shopping area, be redirected to the commercial network to free up more capacity. Via access class barring, new attempts from security guards (not assigned to an

- incident group) are redirected to the commercial LTE network. This decreases the serving eNB load back to 80% (Access Class Barring A.7.1.6.1.1, Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2).
14. IC sets up a secondary perimeter at a 3 mile radius from the incident.
15. The EM notes the perimeter change, and starts the process for a reverse 911 warning call that is sent to all fixed and cellular telephones inside the secondary perimeter. This call instructs the people inside the perimeter to find shelter in the area quickly and to close off all outside ventilation.
- IC creates a second geo-fence and identifies all devices/users in this area. These users are put into a reverse 911 warning call group and a group call is initiated to all in this geo-fenced group (Local Control User Administration A.2.1.3.3.1, Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communications (GCSE 3GPP) A.7.1.5, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3).
  - The on-site dispatcher interfaces with appropriate commercial counterparts to invoke the same reverse 911 warning call to commercial users in the secondary perimeter.
16. The law enforcement branch is directed by IC to coordinate with the Department of Transportation to configure traffic management assets, such as traffic lights and electronic signs, to divert traffic away from the incident.
17. The law enforcement branch has enough assets to establish a perimeter but needs more assets to maintain the security of the incident. IC puts in a request for law enforcement assets to the EM.
- Law enforcement's assets are upgraded to 20 from 10. Law enforcement's elevated profile now contains 20 PTT priority devices/users provisioned in a talk group (10 are added), the same high bit rate HD camera devices, and 5 M2M non-GBR internet/database access devices (fire cameras and M2M sensors) (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communication (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3, Mobile Video Feeds A.7.2.3.1.1).
  - On-site dispatcher software indicates these additional users bring the serving eNB capacity to 90%. No changes are required (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2).
18. The EM begins to coordinate with the public utilities and other pertinent private organizations for the appropriate responses, such as shutting down gas lines to the area and dispatching electrical crews to handle situations, such as downed power lines. The EM also directs additional law enforcement assets into the area upon receiving the request from IC.
- As allocated/assigned additional law enforcement resources enter the perimeter, their priority is raised with a visible flag on their handset (Data Services A.7.2.3).

19. Upon further investigation by law enforcement and fire assets, IC determines that this explosion was not an accident, directs law enforcement to treat the area as a crime scene, and assigns detectives to begin an investigation of the crime scene in coordination with fire investigators. This information is also available to the EM.

20. After determining that the probable cause of the situation is a bomb, IC directs the law enforcement branch to begin directing traffic away from the scene, and to initiate a secondary explosive device search by the Explosive Ordinance Disposal (EOD) team.

21. The emergency medical services branch continues to coordinate the efforts of emergency medical services assets. As casualty information comes onto the command screen via the Radio-frequency identification (RFID) tags used by personnel in the field, the most critical cases are selected for transport to the nearest available hospitals. The emergency medical services branch believes that the on-scene casualties will overburden the medical facilities selected to handle them. The transportation officer is directed to query the local medical facilities regarding their status, capacity for casualties, and what types of casualties can be taken. Casualty statistics are available on demand by IC and the EM. Additionally, the local medical centers coordinate among themselves on resource availability.

- a. EM transfers critical data (RFID tag data, hospital bed capacity and types, to hospital databases) via M2M non-GBR internet secure access elevated priority LTE devices (Data Services A.7.2.3, M2M Feeds A.7.2.3.4).

22. The EM begins to monitor the status of the casualties, as well as the status of the responding medical facilities. Recognizing the casualties from the incident will overburden the nearby facilities, the EM puts a neighboring medical facility on alert for incoming casualties. The EM also directs additional emergency medical services crews to respond to the incident.

- a. As allocated/assigned additional EM personnel enter the perimeter their priority is raised with a visible flag on their handset (Data Services A.7.2.3).
- b. As emergency medical services assets arrive on scene, the assets are registered, and their capabilities are authorized for placement into the emergency medical services asset pool for assignments given by the emergency medical services Branch (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communication (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3, Mobile Video Feeds A.7.2.3.1.1).

24. The unit commander of the EOD team notifies law enforcement that no secondary devices (bombs) have been found. The law enforcement branch pushes this information to IC. IC automatically forwards this information to the EM.

- a. All first responders in law enforcement, fire and emergency management within the perimeters receive a notification via SMS message. (Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3).

25. The fire branch alerts IC that all of the fires have been identified and are marginally contained. Additionally, the hazardous chemical spill has been contained and eliminated by the hazmat teams dispatched by the EM. All but one hazmat team is released back into the regional asset pool.

- a. Via the on-site dispatcher, EM assets/UEs leaving the emergency area are removed from the groups, de-elevating their priority status (Identity Management A.7.1.4, Federated Identity

- Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communication (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3, Mobile Video Feeds A.7.2.3.1.1).
- b. As eNB loading approaches 70%, GBR cameras previously lowered to non-GBR are re-elevated to GBR. M2M-capable cameras are capable of changing their refresh rate and encoding and modulation based on their GBR status and are notified via M2M message of their new bit rate status (GBR or non-GBR) so they can accommodate the new GBR priority class. Access class barring for security guards in the neighboring shopping area is removed so they may access the NPSBN. On-site dispatch software determines these two actions bring the maximum loading to 85% of eNB cell capacity (Data Services A.7.2.3, M2M Feeds A.7.2.3.4).
26. The fire branch alerts IC that all of the fires have been eliminated, and that all but one fire crew has been released back into the regional asset pool.
- a. Via the on-site dispatcher, fire assets/UEs leaving the emergency area are removed from the groups, demoting their priority status (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communication (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3, Mobile Video Feeds A.7.2.3.1.1).
27. The emergency medical services branch alerts IC that all of the injured have been evacuated to appropriate medical facilities. The coroner has been contacted to begin removal of the deceased.
- a. Via the on-site dispatcher, emergency medical services assets/UEs leaving the emergency area are removed from the groups, demoting their priority status (Identity Management A.7.1.4, Federated Identity Management A.7.1.4.2, Support and Define Access Policies A.7.1.4.3, Provide Authorization Services A.7.1.4.4, Support Authentication Services A.7.1.4.5, Dynamic Profile Definition A.4.3.3, Dynamic Incident Management A.7.1.6.1, Static and Dynamic Profiles A.3.4.2.1.2.1, Group Communication (GCSE 3GPP) A.7.1.5, M2M Feeds A.7.2.3.4, Local Control User Administration A.2.1.3.3.1, Instant Messaging A.7.2.3.3.2, SMS/MMS A.7.2.3.3.3, Mobile Video Feeds A.7.2.3.1.1).
- b. With the maximum primary load on the service eNB lower than 40%, on-site dispatch software has determined secondary users may return (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2).
- c. On-site dispatcher software sends an email to the secondary carrier(s) which utilize the spectrum informing them their users may now return to the network. Access class barring is removed and all provisioned users have access. The NPSBN operator sends an explanation of the incident's duration and what actions were taken with respect to secondary users (access class barring, preemption). The NPSBN network should provide detailed records of the logs, data to FirstNet related to resource usage, logging levels and the quality levels (Cloud Services/Hosted Applications A.7.2.3.5, Homepage Situational Awareness A.7.2.3.5.3.1, Network Monitoring A.3.8.3, National Network Operations Center A.3.8.3.1, Network Events A.3.8.3.1.2, Email A.7.2.3.3.1).

#### 4.10.7 Alternative Courses

None identified at this time.

#### 4.10.8 Exceptions

None identified at this time.

#### 4.10.9 Includes

Multi-Discipline/Multi-Jurisdiction-Explosion Scenario use case found in: The SAFECOM Program, “Public Safety Statement of Requirements for Communications and Interoperability”, Volume I, Version 1.2, October 2006.

#### 4.10.10 Special Requirements

1. Outdoor location accuracy consistent with current and future updates to FCC location accuracy policy.
2. Access to IC of third-party floor plans, associated devices, and applications should be available for the first responders

#### 4.10.11 Assumptions

None identified at this time.

#### 4.10.12 Operational Architecture Referenced Functions

Table 5 QPP1, M2M, Secondary Users.4 Operational Architecture References

Operational Architecture Reference	Use Case: QPP1, M2M, Secondary Users.4
A.2.1.3.3.1	Local Control User Administration
A.3.4.2.1.2.1	Static and Dynamic Profiles
A.3.8.3	Network Monitoring
A.3.8.3.1	National Network Operations Center
A.3.8.3.1.2	Network Events
A.4.3.3	Dynamic Profile Definition
A.7.1.10	Location Services
A.7.1.4	Identity Management
A.7.1.4.2	Federated Identity Management
A.7.1.4.3	Support and Define Access Policies
A.7.1.4.4	Provide Authorization Services
A.7.1.4.5	Support Authentication Services
A.7.1.5	Group Communication (GCSE 3GPP)
A.7.1.6	QPP Administration
A.7.1.6.1	Dynamic Incident Management
A.7.1.6.1.1	Access Class Barring

Operational Architecture Reference	Use Case: QPP1, M2M, Secondary Users.4
A.7.1.6.1.2	QCI Management
A.7.1.6.1.5	Incident Command System (ICS) Service
A.7.1.6.1.5.1	Real time Priority and Role Based Execution
A.7.1.6.1.6.1	Immediate Location and Priority Management
A.7.2.1	Mission Critical PTT Voice (3GPP)
A.7.2.3	Data Services
A.7.2.3.1.1	Mobile Video Feeds
A.7.2.3.3.1	Email
A.7.2.3.3.2	Instant Messaging
A.7.2.3.3.3	SMS/MMS
A.7.2.3.4	M2M Feeds
A.7.2.3.5	Cloud Services/Hosted Applications
A.7.2.3.5.3.1	Homepage Situational Awareness
A.7.2.5	Voice Services

#### 4.11 QPP.2: Dynamic QPP Management

This use case includes dynamic priority management of users, services, and applications based upon key triggers that require altering QPP in near-real time.

#### 4.12 User Services.1: Mission-Critical Services

This use case includes Land Mobile Radios (LMR) interoperability, evolution to standards-based Mission-Critical Push-To-Talk (MC PTT), responder emergency situation, immediate peril situation, and a definition of MC data services.

#### 4.13 User Services.2: Proximity Services

This use case includes support for ProSe, GCSE, Direct Mode, and on/off-net communications.

#### 4.14 User Services.3: Cloud Services

This use case includes cloud services including Infrastructure-as-a-Service (IaaS), Software-as-a-Service (aaS), and hosted applications.

#### 4.15 User Services.4: Secondary Users

This use case includes Machine-to-Machine (M2M) services such as meter reading and Closed-Circuit Television (CCTV) collection along with impacts of PS priority and preemption on secondary users.

## 4.16 Network Services.1: Services Delivery Platform (SDP)

This use case describes the overall Services Delivery Platform (SDP) which includes Network Services Platforms (NSP) such as location (including geo-fencing) and presence, broadcast, multi-cast, priority management, and service orchestration.

## 4.17 Network Services.2: Public Safety Enterprise Network (PSEN) Interconnect

This use case includes network interconnect, capacity, test and turn-up, CAD/applications infrastructure networking, and security.

### 4.17.1 Description

The policeman from a local agency is able to use FirstNet to access his PSEN network, a private Internet Protocol (IP) network, to retrieve useful information for his duty. This use case focuses on the interconnection between the FirstNet network and the PSEN.

### 4.17.2 Actors

- Police Officer using a Band 14-capable device, which is provisioned in a communication group
- Dispatcher
- Offending Driver, Suspect
- Back-up Officer using a Band 14-capable device, which is provisioned in a communication group
- Area Supervisor
- Transport Unit Officers
- Booking Officer
- Tow Truck Driver

### 4.17.3 Pre-conditions

1. Officer has completed administrative check-in (A.4, Policies and Procedures).
2. Officer has been issued duty equipment, including a B14 LTE device (A.4.1, Provisioning; A.4.3, User Profile Definition; A.4.4, Billing).
3. Officer's identity and credentials are in local agency database (A.4.2, Network Interop Cert.).

### 4.17.4 Post-conditions

1. Throughout the scenario, the FirstNet network checks the officer's agency network to make sure that this network is not infected with virus or subject to cyber-attacks (A.3.8.2.5.3, Cyber Security; A.3.8.2.5.3.2, Network Monitoring; A.4.5, Best Practice).
2. The network obtains status and information from the Security Operations Center to make sure the access to agency information and network is limited to authorized users and devices. Also, the database in the PSEN is managed in a way that is consistent with the FirstNet security policy. In other words, the PSEN is securely protected (A.7.2.3.5.3.4, Authenticate/Security; A.3.8.2.5.4.1, PS Agency Policy Enforcement).
3. The network maintains secure communications with the PSEN to exchange any suspicious or problematic activities (A.4.6, PS Agency User Security Monitoring).

4. The network provides access control of law enforcement personnel to the PSEN (A.7.1.4.3, Access Policy).
5. The network allows the law enforcement users to define which PSEN they desire to connect with and provides dynamic connection (A.3.8.2.4.3.6, PSEN-interconnection testing; A.7.2.3.5.3.3, Network Status Update).
6. The network provides encryption services including IPSec and sets up VPN tunnels with the PSEN (A.3.8.2.4.3.5, Backhaul-interconnection testing).
7. The network supports both IPv4 and IPv6 (A.7.1.3.1, Domain Name Service).
8. The network, together with the PSEN, tracks the equipment (A.2.1.3.1.4, Diagnostics Monitoring and Management). It also provides criminal information on the arrested suspect and geolocation information in real time to the field supervisor (A.7.2.3.5.3.2, Agency Alerts; A.7.2.3.5.3, Agency Information Home Page; A.3.4.2.9.1, Agency Information Homepage Architecture) as well as dispatchers with the current accountability of all personnel (A.2.1.4.2, Dispatch Center Notified of Critical Outages).
9. All suspect information and evidence are recorded through wireless monitors and voice recognition systems, with no reliance on paper reports and notes (A.3.8.2.5.4.1, PS Agency Policy Enforcement).
10. All information is tagged with the originating officer's identity code (A.7.1.4.2, Federated Identity Management).
11. All evidence is tracked with RFIDs to provide an audit trail (A.1.10.3, Security Auditing).
12. All law enforcement personnel and equipment have monitors to measure vital conditions and status that are reported by the network management system (A.7.2.3.5.3.1, Situational Awareness).
13. National and state criminal justice records and state civilian records are searched and queried via the PSEN database for information relating to the traffic stop (A.7.2.3, Data Services).

#### 4.17.5 Frequency of Use

This situation occurs daily on a nationwide basis.

#### 4.17.6 Normal Course of Events

1. A police officer enters his 10-hour shift at the Brookside jurisdiction. After completing his administrative check-in (A.4, Policies and Procedures), the officer takes his duty equipment to the squad car assigned to him for the shift (A.4.1, Provisioning; A.4.3, User Profile Definition; A.4.4, Billing).
2. In the vehicle, the officer initiates his biometric identity check with his device (A.7.1.4.5.1, Multi-Factor Authentication).
3. This device will first connect to the NPSBN using standard LTE authentication of the IMSI in the device (A.7.1.4.4, Authorization Services).
4. The NPSBN then connects to the policeman's agency network (PSEN), a private IP network, via a VPN tunnel (A.7.1.4.5.2, Single Sign-on).
5. The NPSBN checks the PSEN to make sure that this network is not infected with virus or subject to cyber-attacks. It also obtains status and information from the firewall between the NPSBN and the PSEN, showing the PSEN boundary is securely protected. Throughout the scenario, the NPSBN maintains secure communications with the PSEN to exchange any suspicious or problematic activities (A.7.2.3.5.3.4, Authenticate/Security; A.3.8.2.5.4.1, PS Agency Policy Enforcement).
6. The NPSBN (network) provides access control between the police officer and his selected PSEN. After authenticating the officer, the system sets up a profile of the officer on the device and the network, establishes the level of data access the officer is authorized to have across available

- databases, and initiates tracking of the officer's activities (A.7.1.4.3, Access Policy; A.2.1.3.3, Subscription Management).
7. The officer initiates the equipment self-tests of the devices he will be using within the vehicle. All of the devices code their information with the officer's ID, conduct their registration/authorization steps, and report their status to the wireless network. Each device will be associated with the officer and will provide that officer with capabilities based on the officer's profile. The network communicates with the PSEN and downloads the pertinent database files, the latest law enforcement alerts, and the current road and weather conditions to the device (A.3.4.1.1.3, Device Testing; A.4.1, Provisioning; A.4.3, User Profile Definition; A.4.4, Billing).
  8. After successfully completing all the self-tests, and receiving all the updates, the officer provides a digital status to the network indicating that he has completed all initial setups and is ready. The PSEN reports to the dispatcher, identifying which personnel and equipment are active and available for calls. The officer follows up with a voice call with the same message. The dispatcher acknowledges that the officer is active and that dispatch's GIS and CAD systems are properly receiving location and status data from the officer's vehicle and monitor units (A.3.8.2.4.6.1, Data Analytics; A.3.8.2.4.3.6, PSEN-interconnection testing; A.2.1.3.1.4, Diagnostics Monitoring and Management; A.7.2.3.5.3.2, Agency Alerts; A.7.2.3.5.3, Agency Information Home Page; A.7.1.10, Location Services).
  9. While on routine traffic patrol, the officer observes a car that runs through a red light at an intersection. The officer presses the "Vehicle Stop" button on his vehicle's device. The device issues a message to dispatch via the network and PSEN, noting the operation underway, the officer's ID, and the location information of the officer's car. As the officer drives his squad car, the license number of the offending vehicle is captured by license plate recognition software on the device and sent back for a query to the Department of Motor Vehicles (DMV) via the NPSBN and PSEN. The video camera on the officer's vehicle dashboard begins recording video of the offending vehicle to a device in the officer's vehicle. This video can be accessed at any time, via the network and PSEN connection, by the dispatcher and other authorized viewers. Other units in the area are alerted to the impending vehicle stop (A.7.2.3.1, Video Services; A.7.2.3.1.1, Mobile Video Feeds; A.7.2.3.5.3.2, Agency Alerts; A.3.8.2.5.4.1, PS Agency Policy Enforcement).
  10. Shortly, the State Motor Vehicle Registration, Stolen Vehicle, and Wants/Warrants systems return their information to the vehicle's device via the PSEN and NPSBN. The officer also receives a picture of and information about the registered owner, and whether there are wants/warrants for the owner (A.7.2.3, Data Services; A.7.2.3.1, Video Services).
  11. The offending vehicle pulls over and stops. The video feed will be available to dispatchers and supervisors on demand via the PSEN.
  12. When the officer leaves his squad car, he has access to all of his communications and data devices as the devices continue to communicate between his devices' Personal Access Network (PAN) and the NPSBN and PSEN. The officer approaches the car and notes that there is a single occupant, the driver. The officer requests the driver's license and registration, but the driver does not provide documentation (A.7.2.2, Broadcast Services; A.7.2.3.1.1, Mobile Video Feeds; A.7.2.3, Data Services).
  13. The officer decides to search the suspect's vehicle and contacts dispatch via the PSEN to request a backup unit.
  14. The dispatcher enters the "Dispatch Backup" command for the incident on the dispatch terminal, and the CAD system recommends the dispatch of the closest unit based on automatic vehicle location (AVL) information provided by the vehicles on patrol and known road and traffic conditions. The dispatcher glances at the console map to confirm the recommendation and presses the key to confirm the CAD recommendation. The dispatch of the backup unit is transmitted electronically to

- terminals in that vehicle, as well as to other nearby units and the area supervisor's car for informational purposes, as they are both on the NPSBN and can access to their PSEN.
15. The original and backup officer can communicate and share information, both voice and data, via the NPSBN. The backup officer acknowledges dispatch and asks the on-scene officer to confirm location and circumstances (A.7.2.1, Mission Critical Push-to-talk Voice (3GPP); A.7.2.3, Data Services; A.7.2.2, Broadcast Services).
  16. The supervisor and backup officer bring up the real-time video of the event, which is stored in the video server database in the PSEN, in their vehicles and briefly observe the situation. All appears under control, and they release the video link.
  17. The backup unit arrives on scene. The responding officer orders the suspect to get out of his car. The backup officer watches the driver while the original officer searches the car. The original officer calls dispatch via the NPSBN to request a transport vehicle. The transport unit is dispatched (A.2.1.3.2.3, Storage; A.3.5.6, Data Storage Administration; A.7.2.3.5.3.1, Situational Awareness).
  18. After the arrest, the officer takes the driver's biometric sample with his device. The device sends the scan data to the biometric ID database connected to the PSEN for identification. Soon after, the device receives from the database search an image, name, date of birth, and physical characteristics of the individual from the biometric sample. This indicates that the driver is the registered owner of the vehicle. The officer queries the criminal history database connected to the PSEN for information about the driver and receives a response that the individual has previously been arrested for drug possession (A.7.1.4.2.1, Identify Trust Frameworks; A.7.1.4.5.1, Multi-Factor Authentication).
  19. The officer completes the arrest report in electronic form. The report is transmitted to the officer's supervisor via NPSBN. The supervisor notes one deficiency in the report and issues it back to the officer. The officer corrects the report and retransmits it to the supervisor, who electronically signs off on the report, and forwards it to the Central Records System and to the District Attorney's office, which are connected to the PSEN (A.7.2.3, Data Services).

#### 4.17.7 Alternative Courses

Network Service.2.AC.1                      Related to driver's biometric sample search

1. Insert at Step 11 in Normal Flow.
2. If the vehicle does not belong to the driver, the officer will do a database query of the stolen vehicle database in the PSEN to find out whether this is a stolen vehicle.

#### 4.17.8 Exceptions

None identified at this time.

#### 4.17.9 Includes

1. Traffic stop use case found in: The SAFECOM Program, "Public Safety Statement of Requirements for Communications and Interoperability", Volume I, Version 1.2, October 2006.

#### 4.17.10 Special Requirements

None identified at this time.

#### 4.17.11 Assumptions

None identified at this time.

## 4.17.12 Operational Architecture Referenced Functions

Table 6 Network Services.2 Operational Architecture References

Operational Architecture Reference	Use Case: Network Services.2
A.1.10.3	Security Auditing
A.2.1.3.1.4	Diagnostics Monitoring and Management
A.2.1.3.2.3	Storage
A.2.1.3.3	Subscription Management
A.2.1.4.2	Dispatch Center Notified of Critical Outages
A.3.4.1.1.3	Device Testing
A.3.4.2.9.1	Agency Information Homepage Architecture
A.3.5.6	Data Storage Administration
A.3.8.2.4.3.5	Backhaul-interconnection testing
A.3.8.2.4.3.6	PSEN-interconnection testing
A.3.8.2.4.6.1	Data Analytics
A.3.8.2.5.3	Cyber Security
A.3.8.2.5.3.2	Network Monitoring
A.3.8.2.5.4.1	PS Agency Policy Enforcement
A.4	Policies and Procedures
A.4.1	Provisioning
A.4.2	Network Interop Cert
A.4.3	User Profile Definition
A.4.4	Billing
A.4.5	Best Practice
A.4.6	PS Agency User Security Monitoring
A.7.1.4.3	Access Policy
A.7.1.4.5	Authentication Services
A.7.1.4.5.1	Multi-Factor Authentication
A.7.1.4.5.2	Single Sign-on
A.7.1.10	Location Services
A.7.2.1	Mission Critical Push-to-talk Voice (3GPP)
A.7.2.2	Broadcast Services
A.7.2.3	Data Services
A.7.2.3.1	Video Services
A.7.2.3.1.1	Mobile Video Feeds
A.7.2.3.5.3	Agency Information Home Page
A.7.2.3.5.3.1	Situational Awareness
A.7.2.3.5.3.2	Agency Alerts
A.7.2.3.5.3.3	Network Status Update
A.7.2.3.5.3.4	Authenticate/Security

### 4.18 Network Services.3: Regulatory Services

This use case includes 9-1-1 (legacy PSAP interfaces, NG9-1-1, first responder 9-1-1 dialing and routing), Lawful Intercept (CALEA), and dispatch accuracy to x-y-z location.

### 4.19 Devices.1: Device Ecosystem

This use case includes the full lifecycle of PS devices.

### 4.20 Devices.2: Mobile Device Management (MDM)

This use case includes rooted or jailbreak phone into Equipment Identity Register (EIR), Over-The-Air (OTA) updates, and device configuration.

### 4.21 Devices.3: Bring Your Own Device (BYOD)

This use case includes the process for enabling a user to Bring Your Own Device (BYOD).

BYOD refers to users who Bring Your Own Technology (BYOT), Bring Your Own Phone (BYOP), and Bring Your Own PC (BYOPC). It refers to the policies of permitting employees to bring personally-owned mobile devices (smartphones, tablets, laptops and other such devices) to their workplace, and to use those devices to gain access to their company network, privileged company information and applications.

FirstNet believes that allowing BYOD is not only required to meet the goals of FirstNet's charter but that it will be a means to attract more end users to the FirstNet system. This approach should enable an unprecedented level of device choice and supporting the device ownership model without compromising the security and management the FirstNet system.

#### 4.21.1 Description

FirstNet's BYOD program needs to support and encompass the need for first responders and those that support them to utilize their own devices at either planned or unplanned incidents. This usage should allow for the devices to have as many of the same services as a standard FirstNet device as possible.

#### 4.21.2 Actors

- BYOD user
- Agency user
- Agency administrator

#### 4.21.3 Pre-conditions

1. FirstNet and Contractor confirm the BYOD program meets FirstNet and its end user's needs. (A.3.4.2.2.7.8)
2. The BYOD program shall be supported as needed by the FirstNet systems including: Device Management (DM), Business and Operations Support Systems (B/OSS), core, roaming agreements and similar systems. ( A.2.1.3.1.7, A.2.1.3.1.3, A.1.14)
3. The BYOD program shall be accessible for local control. (A.3.5.1)

- See use case Local Control.1, Services, Applications, Users, and Device Management.
4. The BYOD program records users opt-in and approval status and appropriate documentation (A.2.1.3.1.3), including allowing for their device to be locked and wiped (A.2.1.3.1.6 and A.2.1.3.1.1). Note that a user's request for BYOD support may be allowed or denied (A.3.8.2.3.4.8).
  5. Automatically enforce BYOD specific policies to ensure these devices only access appropriate networks and data if they are compliant (A.3.4.2.2.7.8).
  6. When BYOD devices are entered into the FirstNet systems, they are entered in the FirstNet DM system (A.2.1.3.1.3). This should include the linking of mapping of UICC to a user, user's device, user's subscription and the user agency (A.3.4.2.2.7.9 and A.3.8.2.3.4.9).
  7. The BYOD program allows for the integration and use of devices requiring a Connection Manager (CM) such as PCs with mPCIe, In Vehicle Routers (IVRs) and USB modems (A.2.1.3.1).
  8. Local agencies may adjust their BYOD program with FirstNet and Contractor notification and or consent (A.2.1.3.3, A.2.1.3.1.7).
  9. Tracking and polling of BYOD will be supported by FirstNet's DM system (A.2.1.3.1.3).
    - See use case Devices.2, Mobile Device Management (MDM).
  10. BYOD program is tested and verified to meet FirstNet acceptance per test strategy documentation (A.3.4.2.2.7.8).
  11. BYOD program supports ability for FirstNet and Contractor to maintain updated records for billing purposes and usage tracking. This may include the ability for BYOD devices to be charged or not for services needed used due to extenuating circumstances and tracked (A.3.4.2.2.7.8).

#### 4.21.4 Post-conditions

1. The BYODs on or connected to the FirstNet system are maintained with the most recent updates through the DM system to have the updated versions of FW, SW, Operating System (OS), policy, security and configuration settings (A.3.4.2.2.7.5 and A.3.8.2.3.4.5).
  - See use case Devices.2, Mobile Device Management (MDM).
2. Lost, stolen or devices in question can be placed in a hold status, locked or wiped (A.2.1.3.1.6 and A.2.1.3.1.1).
3. The BYOD program shall allow for the creation and usage of BYOD templates, avoiding the need for a new BYOD setup to be created from scratch (A.2.1.3.1.7).
4. The BYOD program updates and maintains a list of devices or device configurations which can be accepted into the FirstNet BYOD program, this list may also track devices or devices configurations which are not allowed (A.2.1.3.1.3, A.2.1.3.1.7).
5. A BYOD opt-in renew process maybe required. BYODs which have access to the program but have not used the service for extended periods of time may have access removed or placed on temporary hold (A.2.1.3.1.7).
6. The BYOD program evolves as needed to support the evolving needs of FirstNet and its end users. This evolution is supported by FirstNet and the Contractor (A.3.4.2.2.7.8).

#### 4.21.5 Frequency of Use

This situation occurs daily on a nationwide basis.

#### 4.21.6 Normal Course of Events

1. An agency user requests the ability to use a personal mobile device to access his or her agency's communications and data systems through FirstNet (A.2.1.3.1.7).
  - a. The requested device is included on the list of acceptable devices for the FirstNet BYOD program (A.3.8.2.3.4.8).
  - b. The requested device is not FirstNet system capable, or doesn't have Band 14 capabilities. See alternative courses for details as to which features and functionalities BYOD could use depending on the device capability.
2. The user works with his or her agency administrator to follow the process for opting into the BYOD program. The request is accepted, approved and the user's BYOD device is allowed access to the communications and data systems (A.2.1.3.1.7). This acceptance includes having the proper BYOD profile selected to align with the device capabilities and level of access appropriate to the user (A.3.8.2.3.4.8).
  - See use case Applications.1, Identity, Credential, and Access Management (ICAM).
3. The agency administrator logs into the local system to grant access for the user's BYOD (A.2.1.3.3).
4. The user's BYOD begins receiving updates from the FirstNet DM system. This includes being added to the appropriate agency talk and instant messaging groups (A.2.1.3.1.7).
5. The BYOD user (optionally) connects an authorized Blue Tooth (BT) body camera to the user's BYOD and activates video and audio recording / streaming. The agency dispatcher is able to access, view and record the camera's video and audio which is tagged with the user information, location and status (A.7.2.3.1.1).
6. The BYOD user is able to communicate, send and receive information and stay in contact with the other users in the agency. (This communications assumes the current area the user is in has coverage from the provider or other access.) (A.3.4.2.2.7.2 and A.3.8.2.3.4.2)
7. The BYOD user is able to connect the personal device to agency W-Fi system in the office or building locations as well as to In-Vehicle Routes (IVR) and appropriate deployables.
8. The BYOD program includes a container security environment being forced on the device as part of policy, which allows access to needed systems and information but segregates any sensitive data on the device (A.3.4.2.2.7.8). The BYOD program shall allow access in two ways:
  - a. The secure container solution maintains a separation between agency and personal data.
  - b. Secure condition may also include access to agency applications, documents and email through the use of separate applications. (A.2.1.1 and A.3.8.2.4.1.2).
9. The BYOD user views a web page with information he or she wishes to share with an agency user. The BYOD user sees a clickable 'mail to' link in the secure web browser application; the secure mail application handles the request (A.3.4.2.9.1).
10. The BYOD user wants to email the same agency user with additional information on the topic from the web page. The BYOD user selects the agency user contact listed in the agency's directory and in the secure email application. Then the user types up and sends the secure email (A.3.4.2.9.1).
11. The agency user sends the BYOD user a document on the same topic. The BYOD user is able to transfer the document from the email application and store it in the secure application (A.3.4.2.9.1).
12. The BYOD user loses the BYOD device and reports it to the agency administrator. The administrator sends a lock command to the device. The device is still active on a system and sends back a locked received and confirmed notification (A.2.1.3.1.6 and A.2.1.3.1.1).

13. The BYOD user finds the BYOD device and requests that the administrator unlock the device. The BYOD user may also be able to unlock the device by following a special unlock process and codes (A.2.1.3.1.6 and A.2.1.3.1.1).
14. The BYOD user continues to use the device.

#### 4.21.7 Alternative Courses

Depending upon the BYOD device in question and its capabilities, it may or may not have access to certain functionalities and features. The below alternatives detail the potential scenarios.

##### Device.3.AC.1 Related to BYOD without Band 14 capability

1. Wi-Fi
  - a. The BYOD program shall allow for the user device to have voice and data communications over public or private Wi-Fi systems.
2. Over The Top (OTT) communications
  - a. The BYOD program shall allow for the use of OTT applications for data and voice communications between a BYOD device not on the FirstNet system and devices on the FirstNet system (A.8.7.2).
3. Spare device
  - a. In cases where the above alternative courses cannot meet the agency's restrictions or the user's need, the requesting BYOD user can be allotted a spare active and capable FirstNet device (A.2.1.3.1).

##### Device.3.AC.2 Related to BYOD with Band 14 capability

1. Standard usage
  - See use case Devices.1, Device Ecosystem.
2. Real time activation
3. UICC swap
  - a. The FirstNet DM system and BYOD process and procedures should support the user capability of swapping UICC between devices while still allowing for usage on the FirstNet system (A.3.4.2.2.7.9 and A.3.8.2.3.4.9).
4. Spare device
  - a. In cases where the above alternative courses can not meet the need the BYOD program shall support the requesting BYOD user to be allotted a spare active and capable FirstNet device (A.2.1.3.1).

##### Device.3.AC.3 Related to BYOD device lost and not found

1. Agency user sends a command to wipe the secure environment off the device (A.2.1.3.1.6 and A.2.1.3.1.1).
2. The device responds back with receive and confirmed.
3. The device wipes all FirstNet and agency related data from the device. (A.2.1.3.1.6 and A.2.1.3.1.1).

#### 4.21.8 Exceptions

None identified at this time.

#### 4.21.9 Includes

1. Local Control.1, Services, Applications, Users, and Device Management.
2. Devices.1, Device Ecosystem.
3. Devices.2, Mobile Device Management (MDM).
4. Applications.1, Identity, Credential, and Access Management (ICAM).
5. FirstNet's BYOD capabilities needs include but are not limited to:
  - Identity Credentials and Access Management (ICAM)
  - Device Management (DM)
  - Application Deployment and Management – Application Ecosystem
  - Security
  - Network Access In Roaming Situations
  - Approval process for BYOD to access FirstNet services

#### 4.21.10 Special Requirements

FirstNet, Contractor and end users will need to determine the extent to which certain BYOD support conditions are needed as well as which ones are supported (A.3.4.2.2.7.8).

#### 4.21.11 Assumptions (A.3.4.2.2.7.8)

1. BYOD processes and procedures shall support all major and current device operating systems (OS).
2. BYOD processes and procedures will integrate with the selected container technology as needed.
3. BYOD processes and procedures will integrate with FirstNet DM and security systems.
4. The business logic/work flow, for back-end services, is assumed as part of B/OSS domain.
5. Key ancillary systems such as customer service, technical support systems are also assumed to be part of B/OSS domain and are in support of BYOD program.
6. The B/OSS system is the master data keeper of subscriber data including BYOD.
7. Training on the capabilities of FirstNet BYOD processes and procedures is available, updated and distributed as needed.
8. Customer support of the BYOD is available to FirstNet end users per SLA established as an agency or FirstNet end user is on boarded.

#### 4.21.12 Operational Architecture Referenced Functions

Table 7 Devices.3 Operational Architecture References

Operational Architecture Reference	Operational Architecture Function Name
A.2.1.3.1.7	BYOD Management
A.2.1.3.1.3	Device Tracking and Management
A.2.1.3.1.6, A.2.1.3.1.1	Remote Lock and Wipe
A.3.4.2.2.7.4, A.3.8.2.3.4.4	Polling, Diagnostics and Troubleshooting

Operational Architecture Reference	Operational Architecture Function Name
A.2.1.1, A.3.8.2.4.1.2	Security Management
A.7.1.6, A.3.4.2.2.7.10	Quality Priority and Preemption (QPP) and Mobility Management
A.3.4.2.2.7.2, A.3.8.2.3.4.2	Policy and Configuration Management
A.8.7.2	Application (Over The Top (OTT) and Embedded) and Content Management
A.3.4.2.2.7.9, A.3.8.2.3.4.9	Universal Integrated Circuit Card (UICC) Management
A.3.4.2.2.7.5, A.3.8.2.3.4.5	Firmware (FW), Software (SW) and Operating System (OS) updates
A.2.1.3.3.1.3.2, A.2.1.3.3.1.3	Activation and Provisioning
A.3.4.2.2.7.3, A.3.4.2.2.7.6, A.3.8.2.3.4.3, A.3.8.2.3.4.6	Over The Air (OTA) and Tethered Capability
A.3.4.2.2.7.8	Designing and Engineering Enabling Tools and Methods for BYOD Users
A.3.8.2.3.4.8	Updating and Tracking Mobile Devices for BYOD Users
A.1.14	Roaming Administration
A.3.5.1	Local Control Service and User Provisioning
A.2.1.3.1	Device Administration
A.2.1.3.3	Agency User Subscription Management
A.2.1.3.3.1.3	Provisioning of Users
A.7.2.3.1.1	Mobile Video Feeds Service Management
A.3.4.2.9.1	Develop and Manage Agency Information Homepage

#### 4.22 Devices.4: Mobile Communications Unit (MCU)

This use case includes dispatch and the use of a vehicle-based MCU to a rural or remote incident and subsequent arrival of additional responders. MCUs vary based on technical designs and user capabilities.

#### 4.23 Applications.1: Identity, Credential and Access Management (ICAM)

This use case includes federating identities, onboarding agency ICAM systems, and Attribute-Based Access Controls (ABAC).

#### 4.24 Applications.2: Application Development Lifecycle

This use case includes the application developer ecosystem, Mobile Application Management (MAM), Big Data, access to federal, tribal, regional, state, and local incident records databases (DB), security, testing, and certification.

## 4.25 Applications.3: App Stores: FirstNet, Local, Commercial

The FirstNet app store includes publishing, purchasing, billing, settlements, branding, and content management.

### 4.25.1 Description

The first responders from different agencies must be able to discover, browse, purchase and rate the public safety (PS) applications available from the FirstNet app store. In addition, first responders and secondary responders must also be able to access applications on their local app store and on commercial app stores such as Google Play, Apple App Store, BlackBerry World, and Windows Store for certified applications for either FirstNet devices or their BYOD (Bring Your Own Device).

### 4.25.2 Actors

- Local Agency First Responder, Steve
- Federal Agency First Responder, Tom
- Local Agency Dispatcher, Jim
- Secondary Responder (Utility Company), Bill

### 4.25.3 Pre-conditions

1. Steve, Tom, and Bill are all equipped with portable PS B14 LTE UE devices operating within NPSBN coverage.
2. Jim is at the dispatcher location and connected to the Internet and has access to FirstNet.
3. All actors are able to access the FirstNet app store and also the state/agency defined app store (within FirstNet domain). The URL location for FirstNet app store should be available on [firstnet.gov](http://firstnet.gov)
4. The FirstNet users shall be able to purchase the applications using various industry standard payment methods on-line, including their agency charge accounts, major credit cards, PayPal, and other emerging mobile payment systems.
5. The FirstNet app store users shall be able to search for various categories of applications applicable to public safety.
6. The FirstNet users shall be able to discover and search existing commercial stores like Apple App Store, Google Play, Amazon, Blackberry World, Windows Store, and others from the FirstNet app store.

### 4.25.4 Post-conditions

1. First responders are able to download the certified public safety application from the FirstNet app store and are able to successfully install, activate and use it.
2. First responders are able to provide feedback, ratings and other satisfaction measures for the application to the public safety user forum/community available at the FirstNet app store.
3. The payment method (one time or Monthly Recurring Charging (MRC) model) is validated for the downloaded application by the first responder.
4. The on-line records of the downloaded application and purchase transaction are sent electronically to the first responder and to his or her agency account administrator.
5. Application usage is available at the device and also at the network.

#### 4.25.5 Frequency of Use

This situation occurs daily on a nationwide basis.

#### 4.25.6 Normal Course of Events

1. Steve and Tom are attached to NPSBN and able to browse the Internet with their B14 devices.
2. Steve and Tom access the FirstNet app store URL.
3. Steve and Tom view the homepage of the FirstNet app store. The homepage provides the users with various search categories related to public safety applications such as Law Enforcement, Fire, emergency medical services, Alerts, E-911, and others public safety categories. In addition, the users are able to search on device types, payment methods, new releases, and their apps

(Reference to Operational Architecture – A.3.4.2.7.2).

Steve and Tom each search for the law enforcement application category under Police to select and view a specific application's content, description and user ratings.

4. Steve and Jim access their own local agency app store through a redirection from the FirstNet app store. They access, view and download an agency specific application to their agency branded B14 device. The FirstNet app store is able to provide more information of the local catalog such as whether there is any specific application downloadable or embedded, based on the type of device (reference to Operational Architecture – A.2.1.3.1.4.1. and Operational Architecture A.2.1.3.1.4.2).
5. Steve and Jim purchase the application from the FirstNet app store (reference to Operational Architecture A.7.1.7, Operational Architecture A.4.5, Operational Architecture A.2.1.3.3.1.3.2, Operational Architecture A.3.5.4.6, Operational Architecture A.3.5.4.2).
6. Steve and Jim use the application with its included training material that provides a video and a brochure. They also have agency support available or FirstNet customer support via online chat, phone, or email. (Reference to Operational Architecture A.2.1.2, Operational Architecture A.3.4.1.2.1, Operational Architecture A.2.1.3.)
7. Steve and Jim also update another existing application version from the app store. This can be driven from either a FirstNet or agency app version control (Reference to Operational Architecture A.2.1.3.3.1.1).
8. Bill downloads a utility application on his dual-band (B14 with Bx) device from the FirstNet app store. Access to specific first responder applications or agency specific applications is not possible for Bill since he is a secondary responder and is not associated with the local agency (Reference A.1.9, A.6.3).

#### 4.25.7 Alternative Courses

App.3.AC.1 Payments

1. Insert at Step 6 in Normal Flow.
2. The payment method provides customer support Tier 1 service for manual intervention if needed.

#### 4.25.8 Exceptions

None identified at this time.

#### 4.25.9 Includes

1. NPSTC, “Launch Requirements Final SoR”, Rev C, December, 2012.
2. NPSTC, “Local Control Definitions”, Rev F, March 2012.

#### 4.25.10 Special Requirements

None identified at this time.

#### 4.25.11 Assumptions

None identified at this time.

#### 4.25.12 Operational Architecture Referenced Function

Table 8 Applications.3 Operational Architecture References

Operational Architecture Reference	Operational Architecture Function Name
A.1.9	Oversight of Secondary use CLA
A.2.1.2	Customer Service Support
A.2.1.3	Public Safety Entity Management
A.2.1.3.1	Device Administration
A.2.1.3.1.2	Device Policy Apps, Content
A.2.1.3.1.5	Device S/w, F/w Updates
A.2.1.3.3.1.3.2	Rating, Billing Activation
A.3.4.1.2.1	Customer Feedback for long-term services
A.3.4.2.7.2	Design App Store
A.3.5.4.4.2	System Usage Reporting
A.3.5.4.2	Mediation Platform Administration
A.4.1	Define Monitor Implement Provisioning Policies and Procedures
A.6.3	Sales Planning
A.7.1.7	Payment Services Product Lifecycle Management

#### 4.26 Security.1: Rogue App, Malware Detection and Mitigation

This use case includes malware insertion, detection, reporting, isolation, removal, nationwide and regional NPSBN attacks, defenses and controls, whitelisting, blacklisting, and Security Operations Center (SOC).

#### 4.27 Security.2: PSEN Threat Detection and Exclusion

This use case includes monitoring, reporting, network controls, and data loss prevention.

#### 4.28 Operations.1: Network Management

This use case includes network design and architecture, opt-out state interconnect, capacity, coverage, system engineering, service quality management, ticketing, performance management, reporting, and metrics (KPI/SLA).

## 4.29 Operations.2: Network Operations Center (NOC)

This use case includes FirstNet views, state/local views, opt-out state views, fault management, recovery, back-ups, and disaster recovery (DR).

DRAFT