NPSTC

Public Safety Entity Control and Monitoring Requirements for the Nationwide Public Safety Broadband Network

Final Report

October 2015

NPSTC Technology and Broadband Committee

Local Control Working Group

National Public Safety Telecommunications Council

Revision History

Date	Version	Notes	Editor
11-Sep-2015	LC14-07-21	Minor editorial changes and updates (changed tracked and marked with Word comments) for remaining action items from the comment matrix.	Hengeveld
09-Sep-2015	LC14-07-20	Result of 10-Sept-2015 Conference Call	Hengeveld
26-Aug-2015	LC14-07-19	Result of 26-August-2015 Conference Call	Hengeveld
21-Aug-2015	LC14-07-18	Edits for 26-August-2015 conference call	Hengeveld
September 2014	-	Baseline from NPSTC Broadband Working Group, Local Control Task Group: Local Control in the Nationwide Public Safety Broadband Network, Rev F, March 2012.	Hengeveld

Public Safety Entity Control and Monitoring Requirements for the Nationwide Public Safety Broadband Network

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Scope, Origin, and Assumptions

This document is an update to the NPSTC 2012 PSE Local Control and Monitoring Requirements document. The 2015 Working Group reviewed the original document and refreshed the content based on new and emerging technology advances, a more complete understanding of the LTE environment, and clarifications from FirstNet regarding local control and system design.

This report outlines public safety's (PS) needs and expectations for Local Control of the Nationwide Public Safety Broadband Network (NPSBN). It was developed through collaborative discussion by the NPSTC Local Control Working Group (LCWG) and represents the broad consensus of the Working Group. The Title VI of the *Middle Class Tax Relief and Job Creation Act of 2012 (The Act) requires FirstNet to actively consult with public safety about its various needs. This document is NPSTC's input into the consultation process regarding issues of local control.*

For the purposes of this document, a Public Safety Entity (PSE) is defined as federal, state, local, and tribal public safety organizations, that uses communications services from the NPSBN to provide public safety services in response to an incident, unplanned event, or planned event.

Individual PSEs have different needs that vary over both long and short time horizons (i.e., over months or years at the long end, and over minutes and hours within an incident at the short end). Therefore, it is the opinion of the LCWG that flexibility must be built into any Local Control plan. Use of the definitions and requirements herein must not eliminate any particular PSE's flexibility to meet their individual jurisdictional needs and must allow such agencies to adjust their operations and procedures as experience is gained in using the NPSBN. Because many of the PSE needs and requirements reflect the nearer term NPSBN and device capabilities, Local Control requirements will need to be modified as this network and its devices evolve.

1.2 The Dilemma of Local Control

Most of this document is focused on specific requirements for controlling and monitoring aspects of the NPSBN by PSEs. Preliminarily, however, this section discusses our thoughts on adjacent issues related to cooperation and governance.

First, "Local Control" means the ability of PSEs at all jurisdictional levels -- federal, state, local, and tribal -- to configure and monitor their communications systems to adapt to changing mission requirements and system conditions. The phrase "changing mission requirements" denotes a situational continuum ranging from routine to crisis.

Next, the central dilemma of Local Control in a shared network environment is a balancing of the genuine need of PSEs to independently configure their communications with the equally important political and social need to share resources equitably among primary NPSBN-users (i.e., police, fire, and EMS). This is true because the definition of *equitable* is not self-evident. We cannot assume that PSEs comprising an ecosystem of diverse disciplines and jurisdictions will always agree on what constitutes *acceptable inequity* when competing community safety, responder safety, financial, and political considerations are involved.

The resolution of this dilemma requires attention to people, process, and technology including (i) changes in PSE user's perception of *"their"* communications network ("people"); (ii) facilitated inter-agency processes and educational opportunities ("process"); and (iii) technical means for avoiding inefficient use of shared capacity or resources that would cause a negative impact on the network ("technology"). More specifically:

- PSEs joining or subscribing to the NPSBN must accept that they are becoming a part of a community sharing a critical communications resource and that their decisions can have significant impact on other participating entities;
- The First Responder Network Authority (FirstNet[1]), and/or some duly designated proxy, must take a lead role in educating PSEs about technical factors under their control and how they can ensure effective operation of the NPSBN.

  PSEs need to understand, at some level, how applications they deploy and/or use affect the performance of the network as a whole. For example, while many video applications will perform effectively at varying bandwidths, some users may believe the "best" user experience requires very high-resolution video, as with High Definition (HD) video. Were a PSE to naively decide to run all of its video sources at their highest bandwidth at all times, they could significantly impact the overall data load on certain areas of the network and create unnecessary Quality of Service (QoS) issues for other users. By educating PSEs about the impact of various technologies on the network, including best practices, these discussions may encourage PSEs to *condition* their content to make it suitable for the NPSBN.
- FirstNet must facilitate regular dialogue on the best practices and cooperative use of common resources.

  Most PSEs today meet periodically within their community to discuss trends and current events that impact their operations. Those existing community-based public safety forums should be leveraged by FirstNet and/or its contractor(s) to provide an opportunity for regular discussions about NPSBN resources and to gather input from participating PSEs. We also believe that a structured process needs to be established for potential NPSBN PSEs to participate in their community. PSEs need to become aware of the capabilities available to their users as provided by the NPSBN and to identify beneficial applications and services that are utilized throughout their community and the agencies that use them. People engaged in this effort need to agree to come together and work through a structured process, facilitated by FirstNet, to help create an environment in which broadband technology can successfully meet their collective needs.

  Likewise, FirstNet will need to regularly solicit from their PSEs information about their experience using the NPSBN to determine when and if network changes might be needed to facilitate public safety communications.
- Finally, the NPSBN needs to implement the technical means for detecting and managing inefficient use of shared capacity and must provide the technical means by which any PSE can optimize its NPSBN use.

  > Pre-defined plans (i.e., disaster plans) that are established today in Land Mobile Radio (LMR) systems "pre-incident" take into consideration how unique applications and user needs during specific incidents need to be supported and addressed within LMR networks. In the NPSBN, the process envisioned above could provide a forum to determine the priorities associated with different users and applications and would play a critical part of broadband resource policy development. While

[1] It is understood that FirstNet will use contractors and other agents to design, build and operate the NPSBN. These entities are also referred to in other documents and reports as "Broadband Network Operator(s)" or "BBNOs." The term "FirstNet" will be used in this report as the single authoritative entity.

these plans would allow for quicker adjustment of resource priorities, mechanisms should be put in place that allow for individual agency – federal, state, local, and tribal -- input to improve the manner in which controls can be implemented in broadband resource management. Technical controls (e.g., Priority and Quality of Service(PQoS) should be applied in the context of these well-developed resource plans.

Thus, the effective coordination of people, process, and technology is critical to establishing a successful inter-jurisdictional, inter-disciplinary, interoperable, and shared NPSBN. Moreover, smaller PSEs with few resources may have never been required before to access a *shared public safety resource* within their community, where one PSE's use of the resource can have an impact on the resources and quality of applications available to neighboring PSEs. Many PSEs may have neither the ability nor the experience to establish or agree upon Local Control parameters for use of a common resource. Therefore, a regular dialogue on the use of common resources is critical to ensure the right resources are available to the right users, when necessary. In addition, some PSEs may have to learn to co-exist in a community with larger, neighboring PSEs that can utilize more resources and have a greater need to adjust priority and preemption functions.

Other basic elements necessary to address overlapping PSEs/primary NPSBN users include:

(1) Prioritization Availability Awareness. Awareness of prioritization availability by a PSE is directly related to its understanding of applications and users that are presently prioritized in the default use case, what is being prioritized in the present instance by other agencies in their community, and for what purpose. For PSEs to cooperate effectively, they must first be aware of the resources, their limitations, how they are used, and the ability for PSE leadership to prioritize a functionality (or tool) via an application that is agency agnostic -- all to the betterment of the community.

(2) NPSBN Monitoring and Awareness Across PSEs

PSEs need to be aware of the operational status of the NPSBN to make appropriate decisions on the use of resources during times of network congestion. This is especially important because the NPSBN serves and prioritizes multiple applications and services across multiple PSEs. This requires real-time access to information on the overall health of the NPSBN.

PSEs should have access to NPSBN information and performance metrics. PSEs should be aware of the status of the NPSBN and its ability to deliver service to its users. Through Service Level Agreements (SLA), PSEs should be familiar with the baseline capabilities they can typically expect from their applications as they utilize the NPSBN.

(3) Cost Awareness

To account and control for costs, FirstNet needs to provide PSEs with clear and timely subscriber billing information to allow PSEs to control their costs. PSEs must have the ability to retrieve billing data at any time during the billing cycle to monitor costs. At a minimum, the billing system must:

- Provide an electronic billing and accounting portal which will allow easy access to standard and agency customized views of data;
- Clearly identify the rates, usage, and total charges to date;
- Provide easy-to-understand graphical representation of usage for each subscriber or subscriber group;
- Keep billing brief, using plain language descriptions to make charges and usage easily discernible to subscribers;

- Clearly distinguish FirstNet charges from any third-party charges that may be billed through FirstNet to the PSE(s) subscribers;
- Denote any changes in third-party service providers;
- Allow for customized reporting to provide PSEs the ability to retrieve billing data sorted by multiple variables such as date, user classification, etc. and,
- Provide a mechanism to manage and resolve billing and accounting errors.

When FirstNet finalizes its rates structures, these billing information requirements will need to be revisited.

(4) Regional Governance and Cooperation

Resolution of these issues will, at times, require community-based decisions. Communities or regions should have governance processes that will result in mutually agreeable solutions that work for the entire community or region. These solutions will vary by community and cannot be standardized by FirstNet into a one-size-fits-all format. Sharing information about what works and does not will be beneficial, but the ability to develop regional, community-based solutions should remain a key cornerstone of the Local Control requirements.

(5) Service Level Agreements

Many Local Control functions may become integrated into Service Level Agreements (SLAs) that PSEs may enter into with FirstNet. These agreements will likely vary by community and should not be standardized by FirstNet into a one-size-fits-all offering. Service levels such as coverage, throughput, cell edge bandwidth, etc. are proposed topics for discussion in the statutorily mandated State Consultation process, but it is simply too early to determine whether the state plans to be developed by FirstNet will adequately address these issues.

Legacy LMR systems are instructive. Employed by PSEs to provide improved communications for their users and facilitate interoperability, agencies often have their users subscribe to a regional or statewide area radio network that provides system coverage to their jurisdiction. The attributes of such wide-area systems that support multiple agencies are substantial and benefits can be realized to the subscribing agency in the form of improved coverage, improved interoperability, and a certainty of expenses annually for communications services to their agency. These same benefits identified by the PSE resulting from these successful LMR models can be replicated between the FirstNet and the PSEs.

In the NPSBN, where many elements and capabilities will be integrated into applications and services accessed by its primary users, many more variables have to be agreed upon between FirstNet and PSE(s) to ensure the subscribing agency's needs are met. SLAs need to be in place between FirstNet and the PSE to, at a minimum:

- Make evident the degree of service the PSE is expecting is met,
- Be sure the PSE is aware of the applications available to its users within the service and the variance of the parameters supporting such services;
- Provide PSEs awareness of the status of sites providing the service in and around their community; and,
- Ensure those sites operate at a level of service that meets the agreed communications needs established within that community.

Local Control and management of the NPSBN is not confined to fixed infrastructure and resources providing services to NPSBN users within a given community. That is, the NPSBN will also be supporting deployable NPSBN solutions in wilderness, rural areas, and other areas of the country and, therefore, control of these resources must be the purview of the PSE(s) in these areas. Local Control over NPSBN deployable assets should account for (i) the location and storage of equipment, (ii) when and under what conditions the resource will be deployed, and (iii) which agencies will dedicate sufficient personnel and resources to the deployment of these resources. We think these decisions are a necessary part of "Local Control" of the NPSBN.

2 REQUIREMENTS AS IDENTIFIED BY PARTICIPANTS

Overall, the LCWG identified five areas where a PSE will need a span of control with respect to its use of the NPSBN including:

1. Primary NPSBN PSE User and Device Management (Section 2.1) - This section discusses the management and control of subscriptions, applications, and device configurations;

2. **NPSBN Operations and Maintenance** (Section 2.2) – This section describes how the network is operated, monitored, and maintained after it is deployed;

3. General Requirements for Applications and Services (Section 2.3) – This section covers all of the applications and services which utilize the NPSBN;

4. **3GPP Defined Services** (Section 2.4) – This section describes requirements on PSE control of 3GPP defined services currently under development, including Mission Critical PTT Services (MCPTT) and Group Communications Systems Enablers (GCSE); and,

5. **Accounting Requirements** (Section 2.5) - This section describes accounting information required by PSEs.

The following sections provide more specificity for each of these areas of control.

2.1 PSE USER AND DEVICE MANAGEMENT

1. PSEs need a defined span of control over the complete life-cycle of their devices including: PSE subscriptions to the NPSBN;

2. Configuration of PSE subscriptions;

3. Configuration of PSE devices operating on the NPSBN;

4. Applications operating on the device (which is discussed in section 2.3); and,

5. Configuration of the applications operating on the device.

PSEs expect control of devices that their users employ on the NPSBN. A significant portion of PSEs will want their IT organizations to control the configuration of their devices, as is typical of desktop computers and wireless devices they use today.

From a PSE's perspective, a device can be thought of as having two essential management domains affecting the parts of the device. Figure 1 below illustrates the device management domains and the scope of management responsibilities.

The "Agency Device Management Domain" comprises those objects that PSE need to control. These include application clients that are resident on the device and the operational configuration of those applications. Applications include both FirstNet and PSE "Application Layer" objects. Some applications may be controlled by or mandated by FirstNet and therefore out of the control of the PSE.

PSEs should be able to control the security policies, Mobile Virtual Private Networks (VPNs), and other aspects of the Device Operating System particularly those related to unique security requirements that vary on an agency-by-agency basis.

Other aspects of the device, specifically the Subscriber Identification Module (SIM) Card and many aspects of the Device Operating System (OS) and OS configurations are expected to be entirely under the control of FirstNet in order to maintain consistent device behaviors and facilitate interoperability. This element of device management parallels the model of enterprise device management employed by commercial carriers.

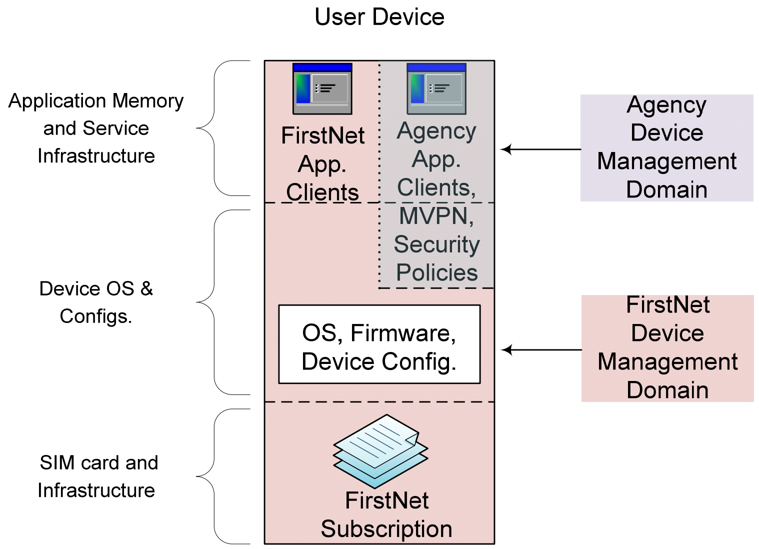
User Device
Application Memory and Service Infrastructure
Device OS & Configs.
SIM card and Infrastructure
FirstNet App. Clients
Agency App. Clients, MVPN, Security Policies
OS, Firmware, Device Config.
FirstNet Subscription
Agency Device Management Domain
FirstNet Device Management Domain

FIGURE 1. USER AND DEVICE MANAGEMENT MODEL

The following sections are intended to articulate and clarify these various managed objects and associated management controls.

- Section 2.1.1 describes PSEs' needs regarding device life cycle management including, in particular, management of device subscriptions;
- Section 2.1.3 enumerates requirements pertaining to PSE management of device configurations, including OS configurations;
- Section 2.1.4 addresses application management; and,
- Section 2.1.4 addresses specific requirements for credential management and related PSE-user configurations.

2.1.1 Subscription Management

One of the elements of Local Control most important to PSE-Users is the ability to decide which users from their agency are authorized to use the NPSBN. In addition to this fundamental requirement, PSEs require the ability to manage the subscriptions of their users (i.e., provisioning, device activations/deactivations, and transfers).

Rather than force end-users to work through a large organization for access to the network, PSEs may prefer to control provisioning and configuration of their devices on the NPSBN. Such control also encompasses which users are authorized to use which devices and applications, which resources users can access, which policies govern the device and user, and how they fit into priority and QoS schema. Because of the dynamic nature of PS operations, the expediency of adding, changing, and deleting devices from the NPSBN is critical. For example, the ability to quickly enable donor devices for hurricane relief or the ability to rapidly remove a stolen device from service is paramount. By controlling the number of devices provisioned or registered on the NPSBN, this capability also provides the PSE-User with the ability to affect charging implications for the agency.

These scenarios are described in more detail below, presented in a situational context, which results in some overlap in support system descriptions.

TABLE 1. SUBSCRIPTION MANAGEMENT REQUIREMENTS

#	Requirements
1	PSEs SHALL have the ability to control when its user devices are changed, added, and deleted from the NPSBN.
2	PSEs SHALL have the ability to manage the device profile in the NPSBN subscriber database.
3	PSEs SHALL have the ability to authorize its NPSBN subscribers to use a device.
4	PSEs SHALL have the ability to manage application subscriptions on each of its devices.

When a PSE-User changes devices or is removed from the NPSBN, controls will be needed to transfer the device from a previous user to a new user without compromising access or security.

TABLE 2. DEVICE TRANSFER REQUIREMENTS

#	Requirements
1	PSEs SHALL be able to transfer devices between users without compromising, access or security.

2.1.2 Life Cycle Management

2.1.2.1 Device Procurement

PSEs must have the ability to choose an approved device and form factor from the vendor of their choice that is best suited to the specific needs of the agency. The NPSBN is envisioned to support a broad spectrum of devices, including modems, smart devices, ruggedized devices, and tablets, to name a few. These devices must support nationwide interoperability as contemplated under the Act as well as the FCC's Technical Advisory Board (TAB) Report.

TABLE 3. DEVICE PROCUREMENT REQUIREMENTS

#	Requirements
1	PSEs SHALL have the ability to choose approved devices that are best suited to their needs.
2	PSEs SHALL have the ability to choose device form factors that are best suited to their needs.

2.1.2.2 Device Inventory and Asset Management

A PSE must have the option of maintaining available inventories of user devices so that it can provide quick replacements and/or bring on new users. Such flexibility will also enable a local agency to provide devices to non-local users who may not have their own devices, and who may be responding to a large-scale incident in the PSE's locale.

TABLE 4. DEVICE INVENTORY AND ASSET MANAGEMENT REQUIREMENTS

#	Requirements
1	PSEs SHALL have the ability to maintain inventories of primary NPSBN user devices.
2	PSEs SHALL have the ability to provide devices to PSEs from other jurisdictions.

2.1.2.3 Activation of New Devices

Device Activation provides the ability to activate an authorized device on the NPSBN for the first time. This service aspect will need requirements relating to time of service delivery and it can be assumed that the local agency will have the new devices ready to be activated.

TABLE 5. DEVICE ACTIVATION REQUIREMENTS

#	Requirements
1	PSEs SHALL have the ability to activate an authorized device on the NPSBN for the first time.
2	SLAs relating to time-of-service delivery for device activation SHOULD be implemented.

2.1.2.4 Replacement of a Lost or Stolen Device

Device Replacement provides for deactivation of an old device and activation of a replacement device. This will depend on service delivery time requirements. PSEs may have spare devices readily available.

TABLE 6. DEVICE REPLACEMENT REQUIREMENTS

#	Requirements
1	PSEs SHALL be able to activate replacement devices.

2.1.2.5 Device Deactivation Control

In a situation in which a rogue user or stolen device is identified, the PSE must have the ability to immediately deactivate the device from the NPSBN. This is similar to the function of radio inhibit in today's radio systems. This service aspect will depend on requirements related to time of service delivery.

TABLE 7. DEVICE DEACTIVATION REQUIREMENTS

#	Requirements
1	PSEs SHALL be able to immediately deactivate lost or stolen devices.
2	PSEs SHALL be able to remotely and immediately lock and wipe a lost or stolen device.

2.1.3 Device Configuration and OS Management

Rather than having to call a centralized help desk for technical support, PSEs must have the option of local technical support services to support their use of the NPSBN. While the expectation is that a PSE would only provide the first level of device management and support, escalation may be necessary. PSEs will require the ability to take advantage of the full range of over-the-air device management capabilities, such as software updating and device health management.

Device management includes aspects of NPSBN configuration, application client provisioning, and application client configuration. Application client configuration aspects are addressed in section 2.1.4. The NPSBN configuration aspects are associated with supported frequency bands, radio access technologies, air interface parameters, and supported features. The application client configuration aspects include authorization policies (e.g., client white lists), OS management (e.g., side-load, download control), security management (e.g., Public Key Infrastructure (PKI) certificate management), and single-sign on/off management. As illustrated in Figure 1, FirstNet should manage the subscription and network configuration aspects, and the PSEs should manage the application client aspects.

2.1.3.1 Over-the-Air Device Capabilities

PSEs would like to have control over the timing of device management (i.e., device software installation, upgrades, configuration changes, etc.) in order to avoid maintenance outages at inopportune times (such as busy hours, sporting events, and major incidents). The NPSBN is further expected to enable many different types of applications and PSEs will want to manage these applications over-the-air (e.g., installation of a common local video client). PSEs must have the ability to perform over-the-air device management capabilities for their devices. Such capabilities include software installation, upgrades, configuration, application management, remote trouble-shooting, and performance tuning.

TABLE 8. OVER THE AIR DEVICE MANAGEMENT REQUIREMENTS

#	Requirements
1	PSEs SHALL have the ability to control the timing of device management software installation, upgrades, and configuration changes.
2	PSEs SHALL have the ability to install, remove, and manage device client applications over-the-air.
3	PSEs SHALL have the ability to perform over-the-air device management capabilities for their devices

2.1.4 Management of PSE Users, their Credentials & Templates

The PSE must have the ability to manage access to applications and services for their individual users. The PSE is ultimately responsible for identifying and credentialing its respective users as part of its public safety administrative responsibility. To simplify the user credential management process, PSEs must be able to utilize existing credential repositories wherever possible. PSEs may at their discretion, choose to have a third-party (e.g. FirstNet Contractor) host a user credential repository for their respective user credentials.

TABLE 9. PSE CREDENTIAL MANAGEMENT REQUIREMENTS

#	Requirements
1	PSEs that manage user credentials (e.g., Username/Passwords, two-factor, etc.) for their respective users within their own organization SHALL be given the option of utilizing these credential repositories to gain access authorization for services and applications hosted by the NPSBN and as well as with other PSEs.
2	PSEs that wish to utilize a third-party user credential repository hosted by a NPSBN authorized entity or by the NPSBN itself SHALL be permitted to do so.
3	PSEs that rely on a third-party user credential repository SHALL retain control of adding, deleting, and modifying user records within the hosted user credential repository through an administrative interface available to each PSE.

2.1.4.1 PSE Control over Individual User Accounts

Rather than require PSEs to work through a large organization for access to the NPSBN, PSEs prefer to control their users' access considering end-user fees, as well as device and other support needs. Such control also encompasses which PSE-Users are authorized to use which devices and applications, which resources users can access, which policies govern the device and user, and how they fit into priority and QoS schema.

TABLE 10. PSE USER ACCOUNT REQUIREMENTS

#	Requirements
1	PSEs SHALL have the ability to control user access to the NPSBN.
2	PSEs SHALL have the ability to control device usage authorization on a per-user basis.
3	PSEs SHALL have the ability to control resource usage on a per-user basis.
4	PSEs SHALL have the ability to control device policies on a per-user basis.
5	PSEs SHALL have the ability to control Priority and QoS schema on a per-user basis.

2.1.4.2 SECURITY POLICIES FOR PSE-USER CREDENTIALS

PSEs need to define and enforce security policies with regard to Identity & Credential Management of users from their respective organizations, subject to a security framework established by FirstNet. Credential Management policies for users must include the ability for the PSEs to choose different forms of credentials (e.g., Username/Password, Two-Factor, PIV-I/FRAC, etc).

TABLE 11. SECURITY POLICIES FOR PSE-USER CREDENTIALS

#	Requirements
1	PSEs SHALL maintain control of their own security policies with regard to the form of authentication used for their respective users, within bounds established by FirstNet.
2	PSEs SHALL be able to choose different forms of user authentication.

2.1.4.3 INFORMATION ACCESS CONTROL AUTHORIZATION

Services hosted by the NPSBN shall utilize access authorization policies appropriate for the NPSBN and as permitted by the security policies of the PSE. Where services and applications of one PSE are hosted and made accessible to other PSEs, the PSE that hosts the service or application shall utilize appropriate access authorization policies as determined by the hosting PSE.

Specifically, this is to state that while authentication of primary NPSBN users may be performed by a PSE or outsourced to a third-party, authorization decisions must *always* be owned by the service provider hosting the application or service.

To enable authorization of NPSBN users by a service provider, a trust framework for PSE identity federation may have to be adopted. A trust framework includes the core technical standards (selection of and profiling of federated access protocols, metadata, trust fabric), and organizational guidelines (governance and legal) to make this capability feasible. The Global Federated Identity and Privilege Management (GFIPM) framework sponsored by the U.S. Department of Justice and the U.S. Department of Homeland Security is an example of one such trust framework.

TABLE 12. APPLICATION AND SERVICE ACCESS AUTHORIZATION

#	Requirements
1	PSEs that host applications and services for users from other PSEs SHALL utilize authorization policies appropriate for the hosting PSE.
2	Resource owners (including FirstNet) SHALL be able to control the minimum authentication strength required to authorize access to their resources.
3	Resource owners (including FirstNet) SHALL be able to authorize access to resources based on relevant attributes of the users identity (e.g., whether the user is a sworn officer) when making authorization decisions.

2.2 NPSBN Operations and Maintenance

NPSBN Operations and Maintenance encompasses those ongoing activities of FirstNet that keep the network operational. Because these activities can have localized effects that can disrupt emergency communications, it is incumbent upon the FirstNet to keep PSEs informed and to consider their input in the planning and execution of maintenance activities. NPSBN Operations and Maintenance solutions need to take shared infrastructure arrangements into account, so PSEs maintain control and access to the network elements upon which their services rely.

2.2.1 NPSBN Monitoring

PSEs must have visibility into NPSBN operations for their users and operational area. Therefore, it is critical that the FirstNet Network Operations Center (NOC) have facilities for relaying appropriate information to PSE operations. Such *read-only* information might include operational status of equipment (up/down).

PSEs' monitoring functionality should include prompt notification to the respective agency of any planned and unplanned outages and any other operationally relevant information regarding use of the NPSBN. In particular, PSEs need the ability to monitor through NOC, and with appropriate restrictions, the fault status of any network sites, equipment, and infrastructure, the failure of which may affect their ability to communicate within their jurisdiction, e.g., a link outage between their network gateway and the controlling EPC.

PSEs should also have the capability to monitor traffic volumes or be notified when network congestion could affect overall system performance. Again, such monitoring need only be read-only through the NOC and may be subject to appropriate access control and other security restrictions.

TABLE 13. NPSBN MONITORING REQUIREMENTS

#	Requirements
1	FirstNet/ BBNO SHALL provide real-time electronic means for PSEs to receive comprehensive fault and status information pertaining to the NPSBN services provided in their jurisdiction.
2	FirstNet/ BBNO SHALL provide real-time electronic means for PSEs to monitor traffic volumes and/or NPSBN congestion pertaining to the services provided in their jurisdiction.

2.2.2 Scheduling for Planned Outages

PSEs must have sufficient mutually agreed advance notice of planned outages within their jurisdictions so that they can develop appropriate communications contingency plans. Likewise, PSEs must be consulted about the timing of planned NPSBN outages, so that they are not scheduled or executed during crucial times. Additionally, PSEs need final *at the moment* authorization so that a planned outage does not interfere with a serious unplanned event in the area that is impacted by services being taken offline.

TABLE 14. NPSBN PLANNED OUTAGE REQUIREMENTS

#	Requirements
1	PSEs with jurisdiction in an affected area SHALL have advance notice of planned outages (e.g., maintenance outages).
2	PSEs with jurisdiction in an affected area SHALL be consulted about the timing of planned outages.
3	PSEs operating in the area of a planned outage SHALL be able to delay the beginning of the outage in order to accommodate serious unplanned events in the affected area.

2.2.3 Real-Time Support

On the NPSBN, some real-time communications parameters will need to be effected by PSEs in order to assure critical communications.

The foremost example of such parameters is the QoS (e.g., admission priority, scheduling priority, packet loss rate, packet latency, etc.) delivered to particular NPSBN users and applications.[2] Whereas the default QoS is expected to be configured in the NPSBN and to be sufficient for normal day-to-day activities, the instantaneous QoS must be flexible to address the needs of emergent events (e.g., incident threatening the life or safety of a first responder). PSEs and primary NPSBN users must have the ability to trigger real-time changes to QoS to meet the needs of the situation.

However, PSEs /primary NPSBN users, including their operational personnel cannot be saddled with directly configuring wireless network parameters. Rather, certain activities (such as pressing the emergency button) must automatically adjust NPSBN parameters so that priority communications continue even in times of congestion.

QoS is one example of a “service affecting parameter” that may require real-time adjustment by PSEs. The following requirements pertain to all such parameters.

[2] See NPSTC’s *Priority and Quality of Service in the Nationwide Public Safety Broadband Network* (http://www.npstc.org/download.jsp?tableId=37&column=217&id=2813&file=PTT_Over_LTE_Master_130719.pdf) for a detailed analysis of public safety’s needs regarding QOS.

TABLE 15. REAL-TIME SUPPORT REQUIREMENTS

#	Requirements
1	PSEs SHALL be able to modify service affecting parameters in real-time.
2	Tools that enable PSEs to modify service affecting parameters SHALL provide operationally relevant views so that PSE personnel need not be experts in the detailed technologies that underlie the service.

2.2.4 PSE Control of Physical Assets

Many PSEs wish to purchase and have operational control over physical assets pertaining to the NPSBN. For example, to enhance coverage or redundancy a PSE may choose to purchase eNodeBs or infrastructure equipment and integrate this equipment with the overall NPSBN. Similarly, PSEs may wish to purchase deployable coverage assets that would need to be integrated into the NPSBN infrastructure. Any physical assets contributed by the PSEs must function as part of the overall NPSBN and be subject to the guidelines negotiated between FirstNet and the PSE.

In the event the NPSBN utilizes physical assets contributed by a PSE, it is understood that the FirstNet's may require logical and or physical management/control/access to those assets; however, provisions should allow for the asset to remain the property of the PSE. The exact nature of the user entity's control of such assets would be subject to agreements between FirstNet and the asset owner. Management of deployable resources by FirstNet contractors must be closely coordinated with local PSEs in order to fully integrate into an efficient response.

TABLE 16. REQUIREMENTS FOR CONTROL OF PHYSICAL ASSETS

#	Requirements
1	The NPSBN SHALL support the integration of PSE owned assets (e.g., eNodeBs) to enhance the coverage, capacity, or redundancy of the NPSBN.
2	The NPSBN SHALL support the integration of PSE- owned deployable assets into the NPSBN.
3	Subject to governing agreements, FirstNet SHALL manage and control PSE owned and integrated assets.

2.2.5 NPSBN Failure Management

Disruptions to backhaul systems, equipment failures at a single site, or catastrophic failure to the core management systems may cause the NPSBN to suffer degraded functionality or to lose service completely. Even minor failures, affecting a single site, can have significant impact on public safety operations. For example, the loss of a communications link during a high-risk incident, such as a house fire, could jeopardize both public safety personnel and civilian safety. FirstNet needs to identify common failure conditions which can impact a single site or an entire region and define the expected system behavior that will be experienced by PSEs during each event. For example, what level of service degradation will be seen at the PSE level following a system failure that disconnects a series of adjacent LTE tower sites?

FirstNet needs to provide a framework for sustained operations at the regional, state, local, and tribal levels during a failure. This framework should include mechanisms to insure real-time monitoring of system and network operational status; real-time notification by FirstNet to PSE designees in the event of a failure; and ongoing communications regarding problem identification, restoration activities, and recommended actions. This will allow PSEs to formalize contingency plans for ongoing public safety operations during times of reduced or absent network access.

TABLE 17. NPSBN FAILURE MANAGEMENT REQUIREMENTS

#	Requirements
1	FirstNet SHALL provide real-time notification (e.g., via email, telephony, or other means) to PSE designees in the event of a service affecting network outage.
2	FirstNet SHALL provide ongoing communications regarding service restoration to PSE designees during service affecting outages.
3	FirstNet SHALL consult with PSE regarding expected failure modes and potential mitigations to support the development of contingency plans for crisis management.

2.3 General Requirements for Applications and Services

Ultimately the purpose of the NPSBN is to enable PSEs to have mobile access to the Internet and software applications that enhance the operational effectiveness of those entities. In particular, these applications include those that allow communications between primary NPSBN users from different jurisdictions that are constrained only by the operational policies of their respective PSE, and not by technical factors. In addition, many PSEs will want to utilize applications hosted within their own PSENs.

The following sections relate to Local Control as it applies generally to applications and services deployed on the NPSBN.

2.3.1 PSENs' Applications and Services

PSEs that are, by definition, local agencies must have access to data sources that are jurisdictionally-relevant or *local* in nature; e.g., local video cameras, floor plans, motor vehicle information, hospital bed counts and specializations, among other information. Such local data and the applications allowing primary NPSBN users to interface with this data are critical for effective use of the network at the local level, and, are in addition to any data sources and applications determined to be required, for nationwide interoperability. Thus, based on appropriate prioritization and a vital QoS framework, such applications and services must be supported, subject to approval procedures as provided by the FirstNet.

The PSE must have the ability to install local applications and services on their associated devices and in their local networks as well as the ability to manage the PSE-User access to those applications.

PSEs utilize specialized multimedia content, such as streaming video from banks, real-time telemetry, and other sources. Also, because of the variable nature of the mission, dynamic prioritization of resources on the NPSBN may become a necessity. For these reasons, the PSE must be provided with the means to define default over-the-air and transport priority and QoS for their applications (subject to the Priority and QoS framework) and the ability to dynamically modify priority and QoS settings as incidents unfold.

TABLE 18. ACCESS TO LOCAL PSE APPLICATIONS AND SERVICES

#	Requirements
1	PSEs that are, by definition, local agencies SHALL be provided access to data sources that are jurisdictionally relevant or *local* in nature.
2	PSEs SHALL be provided a prioritization and QoS framework to support applications which are jurisdictionally relevant or *local* in nature.
3	"The PSE SHALL have the ability to install local applications and services on their associated devices and in their local networks.
4	The PSE SHALL have the ability to manage NPSBN user access to their local applications
5	The PSE SHALL be provided with a means to define default over-the-air and transport priority and QoS attributes for their applications, subject to the Priority and QoS framework.
6	The PSE and NPSBN users SHALL be provided with the ability to dynamically modify priority and QoS attributes as incidents unfold.

2.3.2 Nationwide and Regional Applications and Services

In the same way local PSEs have access to local data resources; the NPSBN must also make available non-local data sources for use to all PSEs. Such sources may include statewide or regional databases and applications, other local data sources outside of an agency's control or nationally interoperable applications and services, such as homepage, Internet, email, IM, and SMS/MMS services.

From a local control perspective, PSE must be able to select from a range of approved database services and applications. Importantly, many PSE already use a wide variety of "over-the-top" applications on commercial networks that meet their current needs. FirstNet should consider and advise public safety on how they will transition from their current applications to the interoperable applications provided by FirstNet and facilitate that transition wherever possible.

TABLE 19. ACCESS TO NON-LOCAL DATA SOURCES

#	Requirements
1	PSE SHALL be able to manage the selection and timing of their transitions from their current applications to those nationwide and regional applications provided by FirstNet.
2	FirstNet SHOULD facilitate transition to interoperable applications through consultation with, and advising of, PSE.

2.3.3 Security and Information Assurance Considerations

The determination of whether an application or service is provided on a nationwide, regional, or local basis should include consideration of security factors.

Moreover, different PSEs may have different requirements and policies that govern their access to the NPSBN. For example, some may wish to have their devices access the NPSBN only through a VPN to services within their control. Others may want access to nationwide services only, with no need for local service access. Others may want access to both nationwide and locally provided services. The NPSBN network must accommodate all three of these operational models.

TABLE 20. APPLICATION SECURITY AND INFORMATION ASSURANCE REQUIREMENTS

#	Requirements
1	PSEs SHALL be able to provide Internet access to their NPSBN users.
2	PSEs SHALL be able to provide and control mobile VPN access through the NPSBN.
3	PSEs SHALL be provided access to nationwide services without dependency on local service access.
4	PSEs SHALL be provided access to locally provided services.

2.3.4 Application Layer Control

Many public safety applications and services have significant administrative and control needs. Many PSEs will require the ability to directly manage mission affecting parameters of applications and services such as the establishment of communications groups, security parameters, keys, etc. Some PSEs with fewer administrative resources should be able to contract with FirstNet to manage applications and services.

For the purposes of the following requirements, an “agency administrator” is an employee (or designee) of a PSE with the authority to modify mission affecting parameters of an application service that is accessible to Primary NPSBN users. Further, an “application service administrator” is an employee (or designee) of the “application service provider” with authority to manage the application service. Without loss of utility, it is assumed that an application service provider could be FirstNet, PSENs, PSEs, or a third party. Mission affecting parameters of applications that are shared across multiple PSEs need to be controlled independently of each other such that one agency’s parameters have little or no impact on the others. Equitable and accountable means for sharing control of mission affecting parameters need to be provided when those parameters themselves are shared between PSEs (e.g., common voice groups).

TABLE 21. APPLICATION CONTROL

#	Requirements
1	Application services SHALL provide a means for remote PSE administrators to manage mission affecting parameters (e.g., group membership) without the need for an intervening third party.
2	FirstNet SHOULD provide a means by which agencies can contract with the BBNO for administrative resources to manage service affecting parameters in their stead.
3	Changes to mission affecting parameters SHOULD, whenever practical, have essentially immediate effect, without the need to restart or take other action at the PSE terminal.
4	Application services SHOULD provide secure API to PSE agency administrative systems to allow agencies to develop custom business systems to modify mission affecting parameters.
5	Application services SHOULD provide a means by which PSE application service administrators can limit or prevent agencies from inadvertently degrading the performance of other agencies sharing the same service platform or transport network.

2.3.5 Management of Installed Applications

PSE agency administrators will need to configure the allowable and required sets of applications available for their users to download. This includes the management of versions as well as the identification of allowed and disallowed applications.

PSE agency administrators may also wish to control the timing of software distribution to ensure reusability when devices are shared between primary NPSBN-users, i.e., multiple first responders and classes of first responders including law enforcement, fire, and EMS. FirstNet should determine how PSE applications are vetted to ensure conformance with security requirements and application development best practices. The NPSBN should track and share logging information which records which applications were downloaded to user devices.

TABLE 22. MANAGEMENT OF APPLICATION INSTALLATION

#	Requirements
1	Agency administrators SHALL have the ability to define the applications (NPSBN deployed, PSEN deployed, or 3rd party deployed) the user is authorized to use, from amongst those approved or otherwise vetted by the NPSBN.
2	Agency administrators SHALL have the ability to change the agency authorized applications and their settings.
3	Agency administrators SHALL have the ability to remove the agency authorization to access an application.
4	Agency administrators SHALL be able to establish or modify agency application authorizations via bulk provisioning mechanisms.
5	Agency administrators SHALL be able to manage the software versions available to their users, if desired.

2.4 3GPP Defined Services

The 3rd Generation Partnership Project (3GPP) is a global standards body that defines and standardizes LTE. Two ongoing areas of standardization in particular concern PSEs using the NPSBN. In the SA6working group, dealing with public safety, specific requirements for services are developed. By statute the U.S. public safety community is represented in these groups by the Public Safety Communications Research (PSCR) program. The following narrative sections provide NPSTC input with regard to two of these important services. Public safety entities should be aware that new and evolved services intended for mission critical use are, even now, being standardized in 3GPP. As these standards are specified and developed, the LCWG and other NPSTC groups will need to continue to provide input periodically to FirstNet about public safety requirements on these services.

2.4.1 PSE Control of 3GPP MCPTT Services

3GPP is in the process of standardizing Mission Critical Push-to-Talk (MCPTT) services for LTE. MCPTT services comprise networked and direct mode PTT communications services as well as user equipment capabilities to relay PTT and other communications between direct mode and networked UE.

Requirements for MCPTT have been extensively enumerated in a previous NPSTC publication.[3] Throughout the requirements enumerated in that document, administration and management requirements[4] are included that describe various specific needs that PSEs have for controlling and monitoring MCPTT services. Those requirements are the baseline for the Local Control needs of PSEs pursuant to MCPTT and we endorse them.

Most of those requirements fall into the class of *mission affecting* parameters discussed in section 2.3.4, above. Because PTT voice is a critical resource of current public safety communications, it is critical that PSEs maintain the same degree of dynamic control over MCPTT that it has over its current systems. These include in particular:

- Management of user profiles that define privileges and group membership of the PSEs users;
- Dynamic management of communications groups that allows PSEs to instantly adapt to changing mission profiles;
- Management of end-to-end security keys and related parameters that affect communications security; and,
- Management of direct mode and relay services.

The following table summarizes the requirements for Local Control of MCPTT services.

[3] *Push-to-Talk over Long Term Evolution Requirements*, National Public Safety Telecommunications Council, 18-July-2013. http://www.npstc.org/download.jsp?tableId=37&column=217&id=2813&file=PTT_Over_LTE_Master_130719.pdf

[4] For example, Table 7 requirement 6 “The PTT Service SHALL provide a mechanism for a PSE Administrator to limit the total number of PTT Group transmission (sic) that a NPSBN user can simultaneously receive.”

TABLE 23. MISSION CRITICAL PTT LOCAL CONTROL REQUIREMENTS

#	Requirements
1	The NPSBN SHALL implement and publish a process that outlines how MCPTT requests are processed and what role PSEs have in ensuring their users are familiar with how the NPSBN processes MCPTT calls.
2	The PSE SHALL have access to individual user's profiles with the ability to modify MCPTT profiles parameters including User Identity, QoS attributes, and Priority levels.
3	The PSE SHALL have the ability to create and manage talkgroups.
4	A PSE SHALL have the capability to control user's access to MCPTT services.
5	A PSE SHALL have the capability to determine which MCPTT user has priority prerogatives in specific talkgroups.

2.4.2 PSE CONTROL OF 3GPP GCSE

The Group Communication System Enablers for LTE (GCSE) architecture is specified in 3GPP TS 23.468. The group communication system is represented by an Application Server using the 3GPP defined enablers for transferring application signaling and application data to a group of devices (i.e., user equipment) either (i) over multicast or broadcast bearer services using the Broadcast Mode of eMBMS[5] (TS 23.246); or (ii) over unicast (EPS) bearers; or (iii) over both eMBMS and EPS bearer services. Further, it is assumed that eMBMS will be used to support the GCSE architecture.

The following paragraphs in this section will describe aspects of PSE control required to establish and maintain eMBMS service areas which are necessary to deliver eMBMS bearer services within the GCSE architecture. An implicit expectation is that the 3GPP defined MCPTT services, as well as other services, will be supported within the GCSE architecture. As such, topics related to PSE control of GCSE are also associated with control of MCPTT service configuration.

An eMBMS Service Area is an area within which data of specific eMBMS sessions are sent. A Multicast Broadcast Single Frequency Network (MBSFN) Area is a set of cells that provide the simulcast transmission within an eMBMS Service Area. Within each cell of an MBSFN, radio resources will need to be partitioned and allocated for unicast EPS bearer services and for eMBMS bearer services. Radio resource partitioning is dependent on the types and volumes of services delivered over these bearer services. As an example, radio resources may be configured to support multiple eMBMS media channels, whereby each media channel could be associated with a group communication, such as a MC-PTT talk group. As such, configuring MBSFN areas can be considered as analogous to configuring LMR site coverage areas. In addition, the amount of radio resources that need to be allocated to an MBSFN area is dependent on other services such as video and data transfer.

[5] Note: There is considerable confusion over the abbreviations "MBMS" and "eMBMS." "MBMS" is sometimes used to refer to the 3G version of Multicast Broadcast Multimedia Services, whereas enhanced MBMS (eMBMS) refers to the 4G version. In this document, "eMBMS" is used, and refers to the 4G version.

The principal PSE control aspects are associated with location and sizes of MBSFN areas and bandwidth requirements for MBSFN areas. Other considerations are media types which will be supported and which eMBMS real-time and/or download delivery modes are required. In shared network scenarios, such as in a public-private partnership, eMBMS resources may need to be shared between commercial consumer services and public safety services.[6]

2.4.2.1 MBSFN AREA PLANNING REQUIRES SIMILAR INPUTS AS LMR SITE PLANNING

MBSFN areas will typically need to be aligned with geographic perimeters of existing jurisdictional communication areas. The reason for this is that public safety personnel typically communicate within their jurisdictional area, and thus communication resources need to be provisioned accordingly. Additional planning may be required at national, regional, local, and tribal levels. As such, PSEs will need to participate in the planning and maintenance of MBSFN areas. PSEs should provide inputs which are relevant to MBSFN area planning including the following:

- Coverage area reliability requirements
- Interference mitigation
- Number of user devices
- Types of services
- Call/usage model for each type of service
- Number of communication groups per jurisdictional area
- System usage characteristics (e.g., support for large events)
- Priority aspects of traffic flows for users and groups of users

TABLE 24. MULTICAST SERVICE AREA PLANNING REQUIREMENTS

#	Requirement
1	PSEs SHALL have the ability to influence the planning of MBSFN service areas to account for their operational needs.

A group is a set of NPSBN users having an ability to simultaneously communicate within the group set. Priority controls and privileges can be applied to individual users, as well as commonly to all users within a group. Thus, a group can inherit the assigned priority attributes of each member of the group, and a group can possess unique priority attributes which are common to all members within the group. The common priority attributes can be used for priority controls and privileges assigned to individual users within the group, as well as priority controls and privileges assigned across multiple groups.

Communications media can be delivered to group members via unicast bearers and/or via multicast bearers. Both unicast and multicast bearers may be delivered over shared resources. In such cases, priority attributes may be used to resolve contention for shared resources. For this reason, priority controls and privileges must be assigned to both unicast and multicast bearers.

[6] This is merely an observation about eMBMS. It is not the purpose of this document to delve into the issues of secondary use.

TABLE 25. GROUP PRIORITY REQUIREMENTS

#	Requirement
1	PSEs SHALL have the ability to influence priority attributes applied to Primary NPSBN user group entities.
2	PSEs SHALL have the ability to influence priority controls applied to Primary NPSBN user group entities.

2.5 Accounting Requirements

FirstNet must provide a variety of accounting services in addition to other core services. PSEs need access to a robust set of data to monitor usage by first responder personnel; track how many devices are in use; track the status of applications downloaded and updates applied; and other information necessary to manage NPSBN resources at the agency level. Information must be presented in a clear and concise way using a web portal or other automated system that will allow the agency to view, manipulate, and report on data elements as required by individual PSE operational needs.

Device management accounting requirements also include the need to track, log, and report on data elements relating to the cost of PSE subscriber devices and services. Information needed by PSEs is allocated into three main groups, Device, Agency, and User, described in the following sections.

2.5.1 Device Accounting

Device Accounting provides the ability to identify and track devices that are owned and operated by a PSE including spare devices, equipment shared among multiple first responders, and other specialized systems including deployable units. A broad range of device usage information should be available to assist the PSE in determining its efficient use. For example, full cost information should be available at the device level.

TABLE 26. DEVICE ACCOUNTING REQUIREMENTS

#	Requirements
1	FirstNet SHALL provide means to facilitate device accounting by PSEs.

2.5.2 Agency Accounting

Agency Accounting provides the ability to identify and track all services and costs assigned to a PSE. It aggregates inventory and invoice information from user and fixed devices to allow a PSE to determine usage and financial impact at the agency level. This includes both one time and recurring costs assigned to the PSE.

TABLE 27. AGENCY ACCOUNTING REQUIREMENTS

#	Requirements
1	FirstNet SHALL provide PSEs with access to summary cost and usage information at the agency level.
2	FirstNet SHALL provide individual PSEs with access to the detailed information on its users and devices that is aggregated into the summary information.

2.5.3 User Accounting

This provides the ability to determine usage information for an individual responder, based on their authenticated user account. A responder may use a device shared among other agency personnel on a shift to shift basis; or may use multiple devices during their tour of duty (example: portable device, in vehicle device, laptop, etc.). To the extent PSEs face charges that are usage based, provisions should be made for the agencies to confirm up-to-date usage information.

TABLE 28. USER ACCOUNTING REQUIREMENTS

#	Requirements
1	PSEs SHALL be able to audit current usage information on a per-user basis.

2.5.4 Additional Considerations

The accounting system should allow a PSE to identify usage and costs incurred across a specific date and time range. Local, state, and tribal PSEs must provide detailed billing records to the Federal Emergency Management Agency (FEMA) to receive reimbursement for expenses incurred during a declared disaster.

It should be noted that FirstNet has not yet identified billing rates and plans. The information in this section may need to be reassessed once billing practices for the NPSBN are established.

TABLE 29. ADDITIONAL ACCOUNTING REQUIREMENTS

#	Requirements
1	In order to accommodate reimbursement of PSEs by FEMA and similar organizations, the NPSBN SHALL provide PSEs with access to usage and cost information across specified date and time intervals.

3 ACRONYMS AND DEFINITIONS

The Working Group has attempted to normalize these acronyms and definitions with those of other NPSTC documents and with related source material; however, not all nomenclature in this report will match other documents.

3GPP

3rd Generation Partnership Program.

Act

Title VI of the *Middle Class Tax Relief and Job Creation Act of 2012.*

Agency Administrator

A PSE's employee (or designee) with the authority to modify mission-affecting parameters of an application service that is accessible to Primary NPSBN-users.

Application Service Administrator

An NPSBN, PSEN, PSE, or 3rd party employee with the authority to manage applications services.

Application Service Provider

Applications provided by the NPSBN, PSEN, PSE, or 3rd party.

BBNO

Broadband Network Operator. An entity or consortium of entities under contract with the federal government to build and operate the NPSBN. Such entities are assumed to be Category 1 National, Category 2 Regional or Hybrid (FN Appendix to Special Notice, Pricing Concepts). The phrase "FirstNet" is used throughout this report as the single point of authority for all actions conducted by the First Responder Network Authority and its contractors.

Consultation

The Act defines "consultation" as: "(i) The process of soliciting, analyzing, and integrating the experience, expertise and related insights of federal, state, local and tribal PSEs for building, deploying and operation of the NPSBN as mandated under Section 6206(b)(1) of the Act. Furthermore, (ii) section 6206(c)(2)(A) mandates consultation with regional, state, tribal, and local jurisdictions with respect to the assignment of priority to local users; assignment of priority and selection of entities seeking access to or use of the NPSBN; and training needs of local users. Finally, (iii) Section 6205(a) of the Act establishes a standing Public Safety Advisory Committee to assist FirstNet in carrying out its duties and responsibilities articulated under Subtitle B of the Act."

Device(s)

A device is an access point to the NPBN that provides direct interfaces for primary NPSBN Users such as a smartphone would or it can be a gateway to the network for another device, such as the modems in vehicles that let mobile data terminal access the network. Devices include, but are not limited, to modems, smart devices, ruggedized devices, and tablets. Also known as User Equipment (UE).

eMBMS

Enhanced Multicast Broadcast Multimedia Service

EPS

Evolved Packet System per 3GPP

FirstNet	First Responder Network Authority, FirstNet or FN, means the independent authority created under the Act that is statutorily charged with the design, construction and operation of the NPSBN.
GCSE	Group Communications Systems Enabler
ICS	Incident Command System as implemented by National Incident Management System (NIMS)
LCWG	NPSTC Broadband and Technology Committee’s Local Control Working Group
LMR	Land Mobile Radio
Local Control	Local Control refers to the ability of PSEs (federal, state, local, and tribal) to configure and monitor their communication systems to adapt to mission requirements and systems conditions.
MBSFN	Multicast Broadcast Single Frequency Network
MCPTT	Mission Critical Push-to-Talk
NIMS	National Incident Management System
NOC	Network Operations Center
NPSBN	National Public Safety Broadband Network, as defined under section 6202 of the Act, based on a single national network architecture and commercial standards that evolve with technological advancements. The NPSBN is dedicated to public safety use and operates on Public Safety Spectrum as set forth under Subtitle A of the Act.
OS	Operating System
PKI	Public key infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Primary NPSBN-User	An entity (PSE) or subscriber that provides public safety services. Inherent in this term is a hierarchy of responder access to the NPSBN referred to as first responder, secondary responder, etc. Currently, first responder refers to police, fire, and EMS organizations whose *entire* organization *always* has priority access to the NPSBN (see, FN’s 3rd Legal NOI).
PS	Public Safety
PSE	Public Safety Entity means a federal, state, local, or tribal public safety organization or agency that makes use of communications services offered by FirstNet for the purpose of provisioning public safety services in response to an incident or planned event.

PSEN

Public Safety Enterprise Network means a network dedicated to public safety users and their specific applications and requirements. PSENs are largely separate from, but are intended to be interconnected with the NPSBN. To avoid confusion with multiple uses of the word “local”, PSEN is employed for reference to so-called *private* PS networks and applications.

PTT

Push-to-Talk

QoS

Quality of Service, Focuses on the quality of the experience attributes (latency, packet loss, etc.) supplied by the broadband network to an application or device

SHALL

The word SHALL is used to identify those items the Working Group considered critical to the success of the NPSBN. In the opinion of the Working Group, the network is unlikely to fulfill its mission and promise if these requirements are not considered.

SHOULD

The word SHOULD is used to identify those items the Working Group considered important to the success of the NPSBN. In the opinion of the Working Group, the network will benefit from including items so indicated.

SIM

Subscriber Identification Module (SIM).

SLA

Service Level Agreement. Note that FirstNet (in the draft RFP) has a specialized definition of SLA. Herein the term is used more broadly.

SOP

Standard Operating Procedure.

TAB Report

Technical Advisory Board Report. Federal Communications Commission, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network,* released May 22, 2012.

UE

User Equipment (see also Device).

VPN

Virtual Private Network.

4 CONTRIBUTORS

NPSTC wishes to recognize the significant involvement of the Local Control Working Group members, including those that participated in the 2012 report and those that contributed to this report, and thank them for their dedication to the project.

Name	Representing	2012	2014
Allen, Karen	State of Arizona		X
Arcuri, Dominick	DVA Consulting		
Baker, Natalie	Intrado		X
Barreto, Edgardo	Puerto Rico Fire Dept.	X	
Bitting, James	Veterans Enterprise Systems Technology		X
Britt, Michael	State of Arizona	X	X
Brouwer, Wim	Alcatel-Lucent	X	X
Burgess, John	Alcatel-Lucent	X	
Carl, Jeffrey	AT&T		X
Cavazos, Robert	Harris County, Texas		X
Chang, Yoon	FCC	X	
Cole, Cynthia	Cynergyze	X	
Coleman Madsen, Kim	State of Colorado		X
Contestabile, John	Johns Hopkins University		X
Crosby, Todd	State of Hawaii		
Daly, Brian	ATT	X	
Davis, Andy	MSI		X
Delatorre, Carlos	NewTel Consulting		X
Devine, Steve	NPSTC		PC[7]
Dolly, Martin	ATT	X	
Doumi, Tewfik	Alcatel-Lucent		X
Eastwood, Jim	MSI		X
Eierman, David	MSI		X
English, Gerald "Jay"	APCO		X
Fischer, Chris	Alcatel-Lucent	X	
Fraser, Barry	BayRICS Authority		X
Galway, Rick	Skylinc Incorporated	X	
Garcia, Victoria	State of Hawaii	X	
Goldsmith, Ron	Plano TX		X
Harrison, Regina	NTIA		X
Hengeveld, Tom	Harris	IC[8]	IC
Horden, Neil	Federal Engineering		X
Johnson, Reid	Harris	X	X

[7] PC = Public Safety Chair

[8] IC = Industry Chair

Jouanelle, Guy	Televate	X	
Kassa, Brian	Kastar	X	
Kennedy, Stephen	Sumter County FL		X
Kindlespire, Chris	Gundy County, IL		
Korinek, Frank	MSI	X	
Kuran, Joe	Washington County, OR	X	
Lefebre, Shawn	Harris		X
Lenihan, John	Los Angeles Country Fire		X
Link, Kenneth	HHS IRCT Communications Specialist		X
Lu, Myles	Star Solutions International		X
Luke, Barry	NPSTC	X	X
Mallory, Steven	State of Maine		X
Militeau, Christian	Intrado		X
Miller, Lester	IYP Solutions	X	
Miller, Trent	MSI		X
Mills, Ed	State of Colorado		X
Montanari, Pam	DHS OEC	X	
Moore, Brian	IAEM; Kelowna (BC) Fire Department		X
Musgrove, Peter	ATT		X
Oprescu, Val	MSI	X	
Pavlak, Bob	District of Columbia (OUC)	X	
Petrea, Bill	APCO International		
Powell, John	IACP		X
Prakesh, Prithu	General Dynamics Canada		X
Raczynski, Mark	General Dynamics		X
Redding, Chris	ITS		X
Richmond, Randy	Zetron		X
Ringqvist, Patrik	Ericsson		X
Ryckman, Mark	State of New York		X
Scribano, Gino	MSI		X
Sennett, DeWayne	ATT		X
Shepherd, Brian	State of Colorado		X
Springer, Bill	Illinois Law Enforcement Alarm Center		X
Sundie, Gregory	State of Arizona		
Sunahara, Alvin	City and County of Honolulu		X
Symons, Bob	State of Wyoming		X
Taillon, Terek	Dane County		X
Todd, Ty	Oklahoma DOT	X	
Tyagi, Dharmesh	Nokia Networks		X
Unruh, Lincoln	RavenTech Corp	X	
Upp, Steve	MSI		X
Wilson, Chris	MSI		X
Wilson, Robert	Wyoming DOT	X	
Wolf, Bill	Elgin, IL Police Department		X