*NPSTC Broadband Working Group*

*Local Control Task Group*

# *Local Control in the Nationwide Public Safety Broadband Network*

Rev F

March 2012

## Revision History

| Date | Version | Notes | Author |
|---|---|---|---|
| 21-Sep-11 | N/A | LC13 Local Control Definition v3 Rev C.docx was the starting point for this document, | Andy Thiessen |
| 27-Sep-11 | v4.0 rev 2 | Not published – Updates from comments matrix (LC18 Rev G) | Tom Hengeveld |
| 30-Sep-11 | V5.0 | Not published – Updated with content, formatting, added cover, open issues. Version for Trent and Tom review | Cynthia Wenzel Cole |
| 03-Oct-11 | V6 | Not published – Changes from Cynthia, Tom, Trent conference call. Preliminary for Tom edit and update. | Cynthia Cole, Trent Miller, Tom Hengeveld |
| 04-Oct-11 | Rev A | Final edits for general release including accepted all markups from v6; addition of "Application Layer Control" to "Applications and Services" section; addition of "Areas for Further Analysis" in Introduction; rewording of definition of "User Entity(ies)" to include federal end users; | Tom Hengeveld |
| 04-Oct-11 | Rev A (clean) | Clean copy (all markups accepted, all comments removed) of rev A. | Hengeveld |
| 17-Oct-11 | Rev B | Revised based on input from 14-Oct conference call. Removed old comments. Changed Title; edits by Trent | Cole, Hengeveld, Miller |
| 26-Oct-11 | Rev C | Final copy edit | Cole |
| 2-Nov-11 | Rev D | Edits made and approved for final release | Cole |
| Feb-12 | Rev E | Changes to 2.2.1 Cell Site Selection, 2.2.2 Site Hardening, 2.2.5 Backhaul Design, 2.3.1 Network Hardening, 2.3.3 Real-time Support, 2.3.4 User Entitiy Control of Physical Assets, and 2.4.4 Application Control in accordance with LC28 Rev B and discussion with Chief Aiken. | Miller, Hengeveld |
| March 12 | Rev F | Removed references to use cases | Hengeveld |

# Local Control in the National Public Safety Broadband Network

## Table of Contents


1 Introduction ..... 4

1.1 Scope, Origin and Assumptions ..... 4

1.2 Areas for Further Analysis ..... 4

1.3 Governance Issues ..... 4

1.4 Definitions ..... 6

2 Requirements as Identified by Participants ..... 7

2.1 User and Device Management ..... 7

2.1.1 Subscription Management: Ability to Change, Add or Delete Devices ..... 8

2.1.2 Device Management ..... 9

2.2 Network Design ..... 10

2.2.1 Cell Site Selection ..... 10

2.2.2 Site Hardening ..... 11

2.2.3 Network Topology ..... 11

2.2.4 Reuse of User Entity IP Network ..... 11

2.2.5 Backhaul Design ..... 11

2.3 Network Operations and Maintenance ..... 12

2.3.1 Network Monitoring ..... 12

2.3.2 Scheduling for Planned Outages ..... 12

2.3.3 Real-Time Support ..... 12

2.3.4 User Entity Control of Physical Assets ..... 13

2.4 Applications and Services ..... 13

2.4.1 Local Applications and Services ..... 14

2.4.2 Nationwide and Regional Applications and Services ..... 14

2.4.3 Security and Information Assurance Considerations ..... 14

2.4.4 Application Layer Control ..... 14

# 1 INTRODUCTION

## 1.1 SCOPE, ORIGIN AND ASSUMPTIONS

The purpose of this document is to outline a User Entity's needs and expectations for its control of a nationwide public safety broadband network. It was developed by the Local Control Task Group (LCTG) of the NPSTC Broadband Working Group through collaborative discussion, and represents, except where noted, the broad consensus of the LCTG.

For the purposes of this document, a "User Entity" is defined to be a public safety organization, be it federal, state or local, that makes use of communications services from a "BB Network Operator" (BBNO). The BBNO could be monolithic (such as a proposed federally created non-profit corporation), or distributed (such as a federation of independently operated regional networks). The distinction between monolithic and distributed governance and operation is not germane to this definition, because this document focuses on the needs of User Entities for control in the PS LTE environment as a whole. Regardless of the operations model, the public safety broadband network is assumed to have licensing and oversight management responsibilities and a mandate to ensure interoperability between the User Entities.

Experience shows that the needs of various public safety agencies are unique and can vary over both long and short time horizons (e.g., 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 LCTG that flexibility must be built into any plan regarding local control. Use of the definitions herein must not eliminate a User Entity's flexibility to meet their local needs, and must allow agencies to adjust their operations and procedures as experience is gained in using the broadband network. More specifically, many of the needs and requirements reflect the nearer term network and device capabilities, therefore the Local Control requirements will need to be modified as the network and devices evolve.

## 1.2 AREAS FOR FURTHER ANALYSIS

This section enumerates topic areas identified by the task group requiring further analysis outside the scope of the task group's charter.

1. The relationship between an over-arching federal authority, in whatever form, and hypothetical regional or statewide networks or network operations requires further definition. In particular, analysis regarding requirements driven by the ability of state, regional or local organizations to implement their own cores is not addressed herein and requires further study.
2. Specific end-user controls (such as the ability to control "remote monitor" and similar functions in a mission critical voice system) are not addressed herein. If, as expected, standards organizations begin to develop interoperable application standards, the detailed control needs of each application should be clearly addressed.

## 1.3 GOVERNANCE ISSUES

During the course of the task group's discussion, the following issues related to governance were identified. The consensus of the group was that, while the governance issues were outside of the scope of its work, they should be captured for further study by an appropriate organization. As such,

this section should not be interpreted as a complete listing of a User Entity's governance needs from the BBNO.

1. Billing arbitration - A formal arbitration and escalation process must be devised for issues pertaining to charging disputes between a User Entity and the BBNO. Arbitration must involve a neutral 3rd party and devices cannot be removed from service without due process.
2. Right of Cancellation - The public safety grade of service requires carefully engineered coverage, fault planning, and customer care. As such, a User Entity may determine a more suitable alternative exists and must retain the right to terminate service from the BBNO at any time.
3. Network Design Arbitration - The User Entity must be provided with a Service Level Agreement (SLA), which identifies expected performance characteristics of the PS LTE network (e.g., bandwidth, coverage, redundancy/availability, quality of service, etc.) In the event that any aspect of the PS LTE network SLA is found to be unsuitable for the User Entity, an escalation process must be defined, which ultimately involves a neutral 3rd party, to seek arbitration.

## 1.4 DEFINITIONS

| | |
|---|---|
| APN | Access Point Name |
| BB Network Operator | This is the entity in control of the monolithic or distributed BB network, possibly a nationwide network governing entity. |
| BB Network | The proposed nationwide public safety broadband network. |
| BBNO | Broadband Network Operator |
| ICS | Incident Command System as implemented by NIMS |
| Influence | Herein, User Entities "influencing" the BBNO is understood to mean that the knowledge and circumstances of the User Entities is actively sought out, considered and accommodated by the BBNO. |
| LCTG | NPSTC Broadband Working Group's Local Control Task Group |
| User Entity(ies) | Federal, state or local organizations that make use of the nationwide public safety broadband network as end users. |
| Must | The word "must" is used herein to identify those items that the task group considered critical to the success of the PS LTE Network. In the opinion of the task group, the network is unlikely to fulfill its mission and promise if these factors are not considered. |
| NIMS | National Incident Management System |
| PS LTE | Public Safety LTE – This refers to a 700 MHz LTE network dedicated to Public Safety use and operating on public safety spectrum. |
| Should | The word "should" is used herein to identify those items that the task group considered important to the success of the PS LTE network. In the opinion of the task group, the network would benefit from including items so indicated. |
| SLA | Service Level Agreement |
| SOP | Standard Operating Procedure |

# 2 REQUIREMENTS AS IDENTIFIED BY PARTICIPANTS

Overall, four areas were identified wherein a User Entity will need some type of control with respect to its first responder's use of a nationwide public safety broadband network, each of which are amplified in the following sections:

1) User and Device Management (Section 2.1) – This involves managing and controlling subscriptions and devices.

2) Network Design (Section 2.12) – This covers all aspects of the infrastructure design including cell site locations, EPC and network backhaul.

3) Network Operations and Maintenance (Section 2.3) – Once the network is deployed, this section describes how the network is operated and maintained.

4) Applications & Services (Section 2.4) – This section covers all of the applications and services which utilize the network.

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

## 2.1 USER AND DEVICE MANAGEMENT

This section pertains to the influence that User Entities have over their subscriptions to the PS LTE network; the configuration of their devices operating on the network; and the configuration of the applications that they employ on the network. Figure 1 illustrates the relationship between these elements. This document assumes User Entities own or possess devices that operate on the PS LTE network by virtue of their subscription to the network.

It seems likely that a significant portion of Agency users will want their IT organizations to control the configuration of their devices, as is typical of desktop computers and wireless devices they use today.

While the section below describes the management of "devices", it should be clarified that a number of the control mechanisms and implementations will apply to a device or will apply to the SIM cards or soft-SIMs. For the purposes of this document the term "device" is used generically to mean either or both depending on the service described.

The following sections are intended to articulate and clarify these various controls.

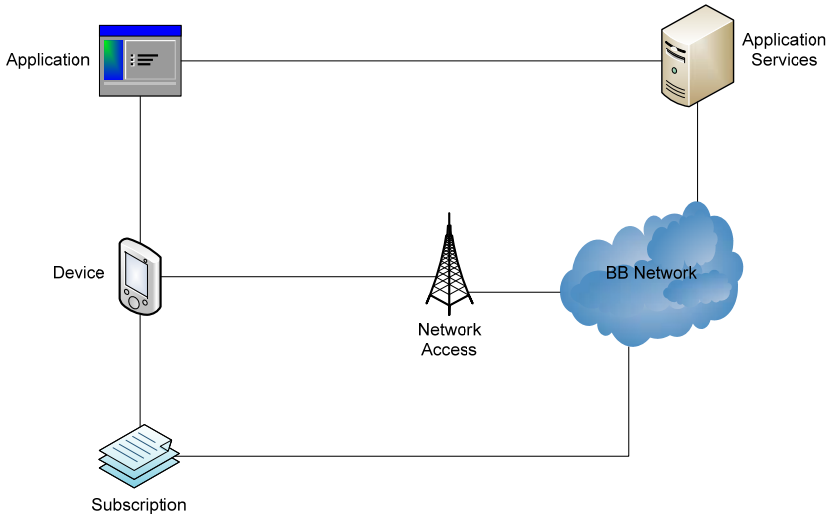


**FIGURE 1 USER AND DEVICE MANAGEMENT MODEL**

### 2.1.1 SUBSCRIPTION MANAGEMENT: ABILITY TO CHANGE, ADD OR DELETE DEVICES

One of the elements of control most important to User Entities is the ability to decide which users from their agency are authorized to use the PS LTE network. In addition to this fundamental need, local agencies require the ability to manage the subscriptions of their users (i.e., provisioning), along with device activations, deactivations and transfers.

Rather than force end-users to work through a large organization for access to the network, local agencies prefer to control provisioning and configuration of their devices on the PS LTE network. 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 Quality of Service schema. Because of the dynamic nature of public safety operations, the expediency of adding, changing, and deleting devices from the PS LTE network 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 PS LTE network, this capability also provides the User Entity 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.

#### 2.1.1.1 DEVICE PROCUREMENT

Local entities must have the ability to choose the device and form factor from the vendor of their choice that is best suited to the specific needs of the agency. The PS LTE network 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 outlined by the regulatory requirements.

#### 2.1.1.2 SUBSCRIPTION MANAGEMENT

This service element provides the User Entity control of device provisioning. In order to meet the dynamic nature of public safety, the User Entity must have the ability to control when User Entity devices are changed, added and deleted from the PS LTE network. This includes management of the device profile in the PS LTE network subscriber database and the ability to authorize responders to use a device. The local agency must also have the ability to manage application subscriptions on each device. For example, access to secure databases should be restricted to authorized applications.

#### 2.1.1.3 ACTIVATION OF NEW DEVICES

This service element should reflect the ability and time it will take to activate an authorized device on the network 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.

#### 2.1.1.4 REPLACEMENT OF A LOST OR STOLEN DEVICE

This service element will require deactivation of the old device and activation of the replacement device. This service aspect will need requirements relating to time of service delivery. It can be assumed that the local agency will have spare devices readily available.

#### 2.1.1.5 DEVICE DEACTIVATION CONTROL

In a situation in which a rogue user or stolen device is identified, the User Entity must have the ability to deactivate the device from the PS LTE network. This is similar to the function of radio inhibit in today's radio systems. This service aspect will need requirements related to time of service delivery.

#### 2.1.1.6 TRANSFER OF USERS ON SAME DEVICE

When an end user is removed from the network, controls will be needed to transfer the device from a previous user to a new user without comprising controls, access or security.

#### 2.1.1.7 MANAGEMENT OF USER CREDENTIALS & TEMPLATES

Public Safety agencies must have the ability to manage individual user access to and credentialing of various database applications and services on the network.

### 2.1.2 DEVICE MANAGEMENT

Rather than having to call some unknown person for technical support, public safety needs local technical support services to support their use of the network. While the expectation is that a local agency would only provide the first level of device management and support, escalation may be necessary. Public Safety 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.

#### 2.1.2.1 USER DEVICE INVENTORY AND ASSET MANAGEMENT

A User Entity must have the option of maintaining available inventories of end-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 User Entity's locale.

#### 2.1.2.2 USER ENTITY CONTROL OVER INDIVIDUAL USER ACCOUNTS

Rather than force end-users to work through a large organization for access to the network, User Entities prefer to control user access to the network considering end-user fees, as well as device and other support needs. 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 Quality of Service schema.

#### 2.1.2.3 ABILITY TO CONFIRM END-USER BILLING INFORMATION

To the extent agencies face charges that are usage based, provisions should be made for agencies to confirm up-to-date usage information.

#### 2.1.2.4 OVER-THE-AIR DEVICE CAPABILITIES

Local entities 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 PS LTE network is further expected to enable many different types of applications and the User Entity will want to manage these applications over-the-air (e.g., installation of a common local video client). The User Entity 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.

## 2.2 NETWORK DESIGN

Historically, User Entities operating on private networks have had nearly complete control over the design, construction and operation of their communications networks. In the context of a nationally-interoperable network operated by the BBNO, that degree of control will potentially be diminished. The following areas, however, are considered by the LCTG to be places where local input is still considered critical to the network design:

### 2.2.1 CELL SITE SELECTION

Knowledge of the local geography[1] is critical to ensuring local agencies have coverage and performance (capacity) where most needed. To that end, the BBNO should consult with User Entities when determining cell site location to influence the BBNO's site design to ensure that areas most in need of coverage and/or high performance, are suitably accommodated. This ability for the User Entity to influence the BBNO must extend beyond the initial design to encompass the design of upgrades and extensions to

[1] Note "geography" is used broadly here to mean physical, political and social geography (including demographics) and including in particularly information about the local deployment and use of public safety personnel.

the network as well. Re-use of existing LMR sites is likely to be desired by both the BBNO and by the owners of the sites (i.e. User Entities). While such re-use may be operationally desirable, reuse of such site would be subject to agreement between the owner and the BBNO..

### 2.2.2 Site Hardening

As the nationwide network is built out, and, as deemed necessary by local agencies, additional, locally funded site hardening should be accommodated when local requirements exceed BBNO's hardening standard, and when such hardening does not interfere with the operation or access required by the BBNO in order to maintain the network. Again, any such modifications would be subject to whatever agreement is maintained between the BBNO and the site owner. Such accommodation will allow local agencies some discretion over sites they deem most critical based on local knowledge, and with the presumption that not all sites will be hardened at the same level as sites funded by the BBNO.

### 2.2.3 Network Topology

Different User Entities of different scale with differing experience with data, and existing public and private networks will have different requirements for accessing applications through the network. The PS LTE network must support at least three different topologies, all with PS LTE over-the-air and transport quality of service:

a) All access from the PS LTE network to the network of the User Entity (e.g., using a private APN or VPN access to route all traffic to the User Entity's own network);
b) All access through network services provided by the BBNO;
c) Some access through local and some through BBNO provided services.

Public safety agencies need the ability to access their existing applications and services through the PS LTE network. Therefore, the network must support interconnection between existing public safety data sources and application services and the nationwide broadband PS LTE network.

### 2.2.4 Reuse of User Entity IP Network

Local entities have existing diverse IP networks (both IPv4 and IPv6) that have been integrated into their workflow. Reuse of these existing networks and applications “as is” will allow for a more gradual transition to the BBN. In order to accommodate variation in existing User Entity networks, the User Entity must be provided with their own LTE APN (Access Point Name). This APN IP space is expected to reuse the User Entity’s existing IP space and thus may be separated from the IP space of the BBNO.

### 2.2.5 Backhaul Design

Because Public Safety has been deploying private voice and data networks for many years, many of them have large amounts of available bandwidth in their existing networks. The BBNO must provide the User Entities with the flexibility to reuse existing backhaul, subject to approval of its suitability by the BBNO, including, in all probability, willingness of the backhaul owner to provide level of service guarantees. Such backhauls may include dark fiber, microwave or MPLS networks. Backhaul reuse should

dramatically drive down backhaul costs, a significant driver in the bandwidth-intensive LTE network design.

## 2.3 Network Operations and Maintenance

Network Operations and Maintenance encompasses those on-going activities of the BBNO to keep the network operational. Because these activities can have localized effects that can disrupt emergency communications, it is incumbent upon the BBNO to keep User Entities informed, and to consider their input in the planning and execution of maintenance activities. Network Operations and Maintenance solutions need to take shared infrastructure arrangements into account, such that PS users maintain control and access to the network elements upon which their services rely.

Several broad areas of communication and control were considered by the task group:

### 2.3.1 Network Monitoring

Local agencies must have visibility into PS LTE operations for their users and operational area. Therefore, it is critical that the BBNO NOC have facilities for relaying appropriate information to the local agencies operations. Such "read-only" information might include operational status of equipment (up/down), and accounting data for their specific users for auditing purposes.

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

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

### 2.3.2 Scheduling for Planned Outages

Local agencies must have sufficient advance notice, as mutually agreed upon, and opportunity to provide input so planned outages are not scheduled or executed during crucial times. Additionally, final “at the moment” authorization shall be required such that a planned outage does not interfere with a serious unplanned event in the local area impacted by services being taken off-line.

### 2.3.3 Real-Time Support

On the BBN, responders are expected to have a default quality of service (e.g. admission priority, scheduling priority, packet loss rate, packet latency, etc.), which will be based on a number of factors, such as the responder’s function and the application being used. This default quality of service is configured into the BBN and should be sufficient for normal day-to-day activities, however it is recognized that the network must be flexible to address serious conditions. User Entities must have the ability to trigger, in real-time,

changes to quality of service to meet the needs of the situation. This does not mean Public Safety responders are expected to directly configure wireless network parameters, rather the act of a responder performing an activity (such as pressing the emergency button) would automatically adjust network quality of service parameters to pre-determined levels (as defined by the national Priority & QoS framework). Triggers to change quality of service will likely involve user/role re-definition as outside users arrive on scene and take responsibility for some part of the incident per NIMS/ICS and local SOPs. Although many quality of service aspects may require and benefit from centralized control, mechanisms will be needed to allow local incident commanders and User Entity administrators to trigger dynamic priority controls without losing valuable time getting necessary approvals. Again, public safety is not expected to directly manipulate BBN parameters; rather trigger the change from a public safety application.

The act of a User Entity triggering a change to the default quality of service for a responder does not require the User Entity to have a complete picture of all activities in the given BBN cell/sector. Rather, based on the conditions at hand a pre-determined dynamic priority value is selected, which will be defined by the national priority and qos framework (e.g. has the emergency button been pressed?).

Also during periods of congestion, the local agency must have the ability to trigger changes to priority and QoS settings for users arriving to assist an agency and operating outside their normal area of control, such as User Entities being able to influence the priority of visiting users.

### 2.3.4 User Entity Control of Physical Assets

Many User Entities wish to purchase, and have operational control over, physical assets pertaining to the BBN. For example, to enhance coverage or redundancy a local entity may choose to purchase eNodeBs or infrastructure equipment and integrate this equipment with the overall BBN. Any physical assets contributed by the User Entities must function as part of the overall BBN and be subject to the same configuration and operational guidelines of the BBNO, subject to governing agreements between the asset owner and the BBNO.

In the event that the national network utilizes physical assets contributed by a User Entity, the BBNO 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 User Entity. The exact nature of the user entity's control of such assets would be subject to agreements between the BBNO and the asset owner.

## 2.4 Applications and Services

Ultimately the purpose of the nationwide Public Safety LTE network is to enable User Entities to have mobile access to software applications that enhance the operational effectiveness of those entities. In particular, these applications include those that allow communications between users from different jurisdictions that are constrained only by the operational policies of their respective entities, and not by technical factors. In addition, many User Entities will want to utilize "private" applications hosted within their own networks. The task

group explored the following broad areas related to application control in the broadband network:

### 2.4.1 Local Applications and Services

Local agencies must have access to data sources that are local in nature such as local video cameras, floor plans, motor vehicle information, hospital bed counts and specializations, among other information. Such local data and the applications allowing users to interface with this data, are critical for effective local use of the network, 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 quality of service framework, such applications and services must be supported, subject to approval procedures as provided by the governing entity.

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

User Entities 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 PS LTE network may become a necessity. For these reasons, the User Entity 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.

### 2.4.2 Nationwide and Regional Applications and Services

In the same way local agencies have access to local data resources, the nationwide network must also make available for use non-local data sources. 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.

### 2.4.3 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. For example, it may be more secure to provide internet access locally to limit the scope of access to public safety devices should the national network ever be compromised by an attacker.

Moreover, different User Entities may have different requirements and policies that govern their access to the network. For example, some may wish to have their devices access the network 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 nationwide network must accommodate all three of these operational models.

### 2.4.4 Application Layer Control

It is anticipated that many public safety applications and services will have significant administrative and control capabilities. Local entities must have the ability to directly manage mission effecting parameters such as the establishment of communications

groups, security parameters and keys, and so on. Local entities should be able to contract with the BBNO to provide management services for their hosted services.