



**Public Safety
Spectrum Trust**

November 30, 2007

To Prospective D Block Bidders:

On behalf of the Public Safety Spectrum Trust (PSST) Board of Directors, thank you for your continued interest in public safety's vision and needs regarding a Public/Private partnership to create a shared, wireless broadband network involving the D Block in the Federal Communications Commission's (FCC) Auction 73. On November 15, 2007, the PSST Board of Directors released version 1.0 of the Bidder Information Document (BID v1.0), which was intended to provide prospective D Block bidders with information about certain PSST expectations and preferences with respect to the Public/Private partnership. The information was released to help prospective D Block bidders formulate their bidding strategies based on public safety's general service needs. Since release of the BID v1.0, the Federal Communications Commission granted the PSST the single nationwide license for the public safety 700 MHz spectrum on November 19, 2007. As you are aware, these matters, along with many other references and input, will be addressed in the Network Sharing Agreement negotiation process with the D Block winner. The PSST reiterates to all prospective D Block bidders its commitment to engage in good faith negotiations consistent with its responsibilities to the public safety community.

Since release of the BID v1.0, the PSST has continued to meet with prospective D Block bidders and, in particular, to seek feedback about this document. The overall reaction from prospective D Block bidders and others has been overwhelmingly positive. Based on the responses, a number of sections to the BID v1.0 have been revised and these changes can be read easily in the red line of the BID v2.0. The PSST is simultaneously releasing red line and clean versions of the BID v2.0. The changes address the following issues: (1) the ability for public safety to join the network through normal commercial channels, without priority, if desired; (2) the spectrum lease payment; (3) priority service for commercial users; and (4) calculation of the wholesale rate. These changes are intended to clarify rather than alter the fundamental principles of the BID. The BID v2.0 is the final, official document from the PSST addressing these issues prior to the start of the 700 MHz spectrum auction on January 24, 2008.

Over the past months public safety organizations have spent considerable time creating recommendations about potential D Block network requirements. Their ideas, dedication, commitment and feedback are much appreciated by the PSST. Likewise, the PSST appreciates the strong interest and feedback from prospective D Block bidders. The PSST looks forward to negotiating with the D Block high bidder to create a

Public/Private partnership that will result in a shared, wireless broadband network that will benefit all Americans.

Sincerely,

Harlin R. McEwen
Chairman



**Public Safety
Spectrum Trust**

***Public Safety Spectrum Trust
Public/Private Partnership
Bidder Information Document***

Bidder Information Document Revision History

Version	Date Released
1.0	11/15/07
2.0	11/30/07

Table of Contents

1	Introduction	3
1.1	Purpose and Background	3
1.2	Bidder Information Document Content.....	3
1.3	Conformance to Applicable Rules	3
2	Technical Issues	4
2.1	Background	4
2.2	Public/Private System Architecture.....	4
2.3	Network Technology Platform	6
2.4	Network Coverage	7
2.5	Network Reliability, Availability, and Hardening	9
2.6	Network Capacity.....	10
2.7	Network Security and Encryption.....	10
2.8	Network Priority and Quality of Service (QoS)	11
2.9	Operational Capabilities - Network Services and Applications	13
2.10	Operational Control - Public Safety Command and Control.....	15
2.11	Public Safety Device Selection and Satellite Devices	16
3	PSST and D Block Winner Partnership Relationship.....	18
3.1	PSST Ownership Position	18
3.2	PSST Rights to "Priority Services" and Public Safety Users.....	19
3.3	PSST Management of Public Safety User Access Rights and Privileges	20
3.4	PSST SWBN Wholesale Rates	21
3.5	Spectrum Lease Payment	26
3.6	Coincident Market Launch of Commercial and Priority Services	27
3.7	PSST Device/Service Expeditious Testing and Approval	27
3.8	PSST Economies of Scale	28
3.9	Satellite Services and Devices	29
4	Appendix A Glossary / Acronyms	30

1 Introduction

1.1 Purpose and Background

This Bidder Information Document (Version 2.0) was prepared by the Public Safety Spectrum Trust Corporation (PSST). It responds to requests from prospective D Block bidders seeking additional high-level information regarding the PSST's expectations of the D Block partner in building and operating the shared Public/Private network described in the FCC's Second Report and Order governing the 700 MHz band.¹ Moreover, this document is intended in part to define and detail certain expectations that the PSST has for this partnership. The PSST expects that the positions that it has developed and presented in this document will form the basis for its negotiation of the affected parts of the Network Sharing Agreement (NSA) that will be negotiated with the D Block winner at the completion of the 700 MHz auction. It is intended to assist prospective bidders in building their business plans prior to the auction in order to minimize significant differences in expectations between the D Block winner and the PSST in the NSA negotiation process. This is the final version that will be released prior to Auction 73.

December 3, 2007 is the FCC Form 175 application filing deadline for Auction 73. From this date until after the auction has closed, the PSST is not planning to communicate directly with prospective bidders, although it may provide additional information publicly if prospective bidders identify areas where such information is needed and it can be appropriately provided in a manner that does not raise concerns under the FCC's anti-collusion rules.

1.2 Bidder Information Document Content

This Bidder Information Document was developed to present certain key technical and non-technical elements that the PSST expects to be incorporated into the NSA. The first section of the document describes certain technical expectations for the network. The second section describes the PSST's preferences regarding certain key business and partnership relationships that are relevant to the shared Public/Private network structure.

This document is not intended to cover all elements that will comprise the NSA. Rather it focuses on certain areas that have been identified by the public safety community and prospective bidders as being among the essential components of the NSA.

1.3 Conformance to Applicable Rules

This document and the position and views that the PSST express are conditioned on compliance with the FCC rules and policies governing the Public/Private partnership adopted in the Second R&O including those relating to the construction and operation of the Shared Wireless Broadband Network (SWBN) to be deployed pursuant to that partnership.

¹ *Second Report and Order*, FCC 07-132, rel. Aug. 10, 2007 ("Second R&O").

2 Technical Issues

2.1 Background

The FCC's Second Report and Order establishes a "minimum" set of technical requirements for the SWBN.²

These requirements form the basis for the PSST's discussion of its expectations for a public safety grade SWBN.

2.1.1 Discussion Topic Areas

The areas to be addressed within the technical section of this document are as follows:

- (1.) Public/Private System Architecture
- (2.) Network Technology Platform
- (3.) Coverage
- (4.) Network Reliability, Availability and Hardening
- (5.) Capacity
- (6.) Security and Encryption
- (7.) Network Priority and Quality of Service (QoS)
- (8.) Operational Capabilities - Network Services and Applications
- (9.) Operational Control - Public Safety Command and Control
- (10.) Public Safety Device Selection and Satellite Devices

2.2 Public/Private System Architecture

2.2.1 Background

Public safety entities have traditionally managed and operated their own communications systems. As functional areas of operation migrate to the SWBN (e.g. Radio Access Network, Transmission, Core Network), PSST-designated Public Safety Users³ expect that, through the PSST, some operational elements will remain within their control and/or there will be a level of agreed upon visibility into the state and health of the network and services delivered to those users via the SWBN.

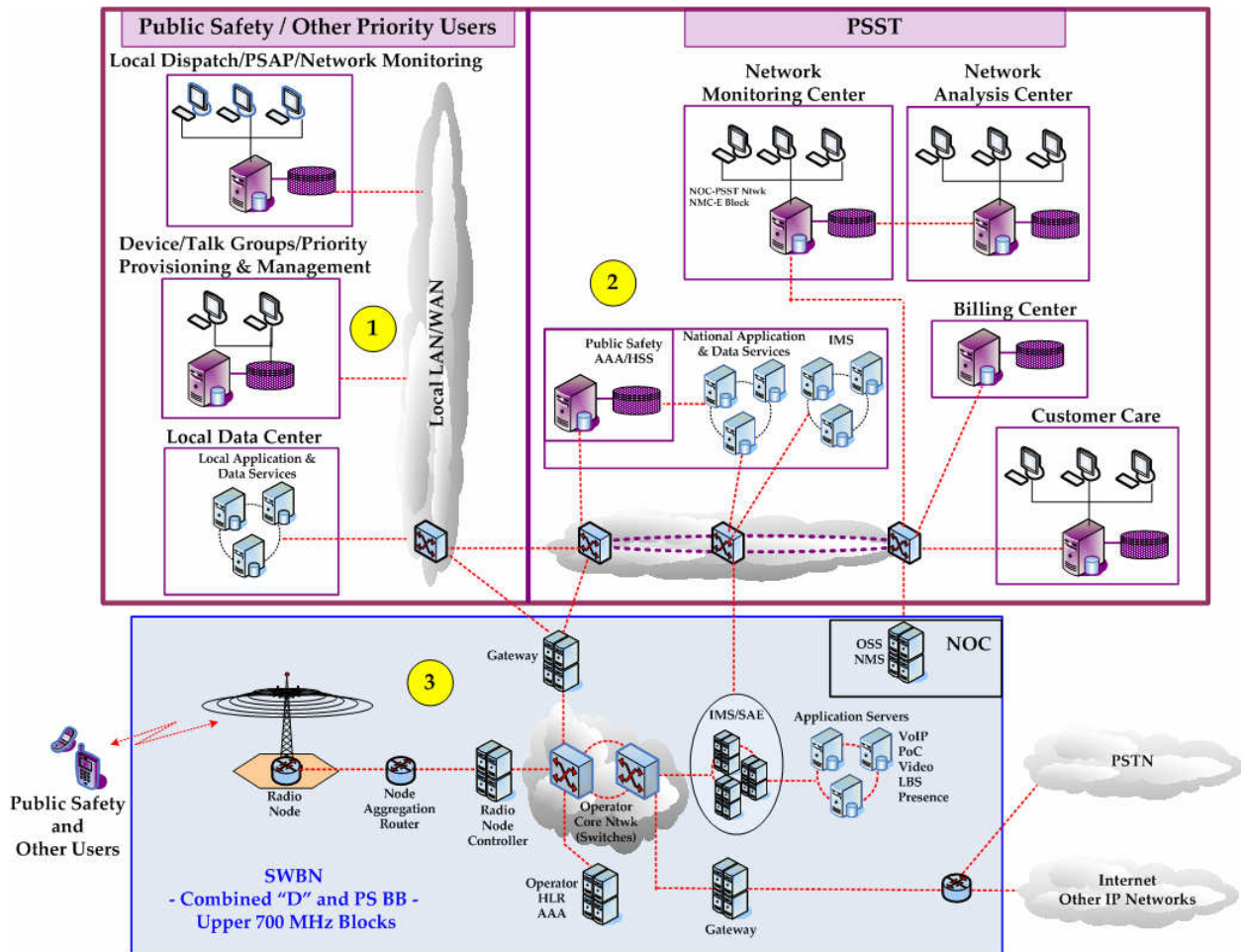
² Second Report and Order at ¶ 405. See also 47 C.F.R. § 27.1305 and § 90.1405.

³ In light of its intended roles and responsibilities, the PSST expects to occupy a meaningful "ownership" position, giving it direct involvement with respect to all public safety and, subject to FCC approval, other PSST approved users such as Federal public safety ("Public Safety Users") on the national SWBN. See Section 3.1(1) herein.

2.2.2 Functional Elements

Figure 2.2.2-A provides an illustration of the functional and technical inter-connection, inter-networking arrangements, and topology that is envisioned to support the PSST's objectives and operational requirements.

Figure 2.2.2-A Public/Private Network and Systems Functional Topology



As shown in Figure 2.2.2-A, there are three functional topologies that comprise the Public/Private partnership arrangement. They are:

- (1.) Public Safety Systems
- (2.) PSST Systems
- (3.) SWBN and Support Systems

With a systems topology such as this, public safety will be able to perform over-the-air updates to devices, allow for access to external and local databases and networks, have access to subscribers' user status, and have the ability to create, modify, delete, and update user and group records, profiles and configurations. Lastly, public safety has a strong need to have levels of visibility into the status of the network to ensure, at a minimum, the health and safety of public safety should SWBN communications be impacted.

2.3 Network Technology Platform

2.3.1 FCC Rule

§ 27.1305 (2)(a) / § 90.1405 (2)(a)

The Shared Wireless Broadband Network developed by the 700 MHz Public/Private Partnership must be designed to meet requirements associated with a nationwide, public safety broadband network. At a minimum, the network must incorporate the following features:

- (a) Design for operation over a broadband technology platform that provides mobile voice, video, and data capability that is seamlessly interoperable across public safety local and state agencies, jurisdictions, and geographic areas, and that includes current and evolving state-of-the-art technologies reasonably made available in the commercial marketplace with features beneficial to the public safety community.
- (b) Sufficient signal coverage to ensure reliable operation throughout the service area consistent with typical public safety communications systems.
- (c) Sufficient robustness to meet the reliability and performance requirements of public safety.
- (d) Sufficient capacity to meet the needs of public safety.
- (e) Security and encryption consistent with state-of-the-art technologies.
- (f) A mechanism to automatically prioritize public safety communications over commercial uses on a real-time basis consistent with the requirements of § 27.1307.
- (g) Operational capabilities consistent with features and requirements that are typical of current and evolving state-of-the-art public safety systems.
- (h) Operational control of the network by the Public Safety Broadband Licensee to the extent necessary to ensure that public safety requirements are met.

2.3.2 PSST SWBN Technology Platform Expectations

- (1.) The formal technology selection and upgrade and migration plans will be negotiated as part of the NSA. Multiple technologies are viable, assuming public safety's requirements are met, and the ultimate technology choice, is expected to, in large part, depend on the auction winner and adoption of open standards.
- (2.) The SWBN technology platform will be based, wherever possible, on commercial off the shelf (COTS) technology that provides mobile data, video and cellular voice capabilities that are seamlessly interoperable across agencies, jurisdictions, and geographical areas.
- (3.) The SWBN technology platform should provide cellular Push-To-Talk (PTT) capability to be used as back-up for mission critical land mobile radio networks. The preference is to have the cellular PTT capability available at network launch.
- (4.) The SWBN technology platform will use a single common air interface (CAI) and the CAI shall allow migration to future technology upgrades.
- (5.) The technology selected for the SWBN will evolve and be upgraded based on commercial wireless upgrade timeframes; however, future upgrades should be backward compatible allowing for appropriate transition periods so that devices do not become obsolete.
- (6.) The PSST and the D Block winner will establish a joint program to identify public safety user requirements affecting the network technology road map and support the appropriate standards development organization's (SDO's) process to make those requirements part of subsequent technology releases.

- (7.) The SWBN should launch with, and/or upgrade to, a uniform, IP Version 6 as required based on Federal government mandates.

2.4 Network Coverage

2.4.1 FCC Rule

§ 27.1305 (2)(b); § 90.1405 (2)(b); § 27.14(m)(1)

Sufficient signal coverage to ensure reliable operation throughout the service area consistent with typical public safety communications systems.

2.4.2 Build-Out Milestones

The FCC has identified the following build-out milestones:

Year 4 –	2013	75% population coverage
Year 7 –	2016	95% population coverage
Year 10 –	2019	99.3% population coverage

Communities in excess of 3,000 people are part of the build-out, as well as all major US highways and interstates.

2.4.3 PSST SWBN Coverage and RF Reliability Expectations

- (1.) The method for calculating coverage will be negotiated as part of the NSA, but it is expected that signal levels will be sufficient to provide the RF reliability, as defined in 2.4.2 (2) below, to ensure coverage consistent with public safety's operational requirements.
- (2.) It is expected that markets should begin launching no later than the first quarter of 2010 and population coverage will increase on a regular basis so as to meet the FCC milestones consistent with a 10 year market roll out plan that will be jointly agreed to in the NSA.
- (3.) The market plan will be subject to an annualized joint review process as informed by input from all levels of public safety entities and should include provisions for enhanced coverage for difficult areas.
- (4.) Signal Reliability
 - (a) The SWBN should provide seamless coverage (via handoff/handover mechanisms) and continuous connectivity with a 95% signal level reliability over 95% of an area as defined by county, township, or parish boundaries at stationary and vehicular speeds up to 75 miles per hour (120 km/h).
 - (b) Table 2.4.2-A (below) is provided to assist in determining average cell site radii per morphology class.
 - (c) Table 2.4.2-A also represents anticipated data rates through the first 4 years of operation, with incremental improvements consistent with overall commercial industry throughput improvements, expected with time.

Table 2.4.2-A

Morphology	<i>In-Building Penetration Margin</i>	<i>Coverage Availability</i>	<i>Sector Loading</i> Sector is loaded to this level of traffic	<i>Forward Link Throughput</i> <ul style="list-style-type: none"> • On-street • Single user • Average cell edge throughput 	<i>Reverse Link Throughput</i> <ul style="list-style-type: none"> • On-street • Single user • Average cell edge throughput
Dense Urban	22 dB	95%	70%	1000 kbps	256 kbps
Urban	19 dB	95%	70%	1000 kbps	256 kbps
Suburban	13 dB	95%	70%	512 kbps	128 kbps
Rural	6 dB	95%	70%	512 kbps	128 kbps
Highway	6 dB	95%	70%	128 kbps	64 kbps

(d) Table 2.4.2-B below represents the parameters the PSST used for defining morphology classes.

Table 2.4.2-B

Morphology	<i>Population Density Based on County Boundaries (pops/sq mile)</i>	<i>Area Description</i>	<i>Approximate Land Mass (sq mile)</i>
Dense Urban	+15,000	Skyscrapers, high rise apartments, buildings of 20+ stories, narrow streets	297
Urban	2,500 – 14,999	Hotels, hospitals, buildings of 4-19 stories, medium to narrow streets	12,367
Suburban	200 – 2,499	Buildings of 1-3 stories, trees and foliage, medium width streets	258,380
Rural	0 – 199	Large open spaces, isolated highways, 1 -2 story houses, barns	3,268,719
Highway	NA	Stretches of interstate highway, and/or US highways, principally within under-populated areas	NA

2.5 Network Reliability, Availability, and Hardening

2.5.1 FCC Rule

§ 27.1305 (2)(c); § 90.1405 (2)(c)

Sufficient robustness to meet the reliability and performance expectations of Public Safety.

Second R&O Para 405

Sufficient robustness to meet the reliability and performance expectations of Public Safety. To meet this standard, network specifications must include features such as hardening of transmission facilities and antenna towers to withstand harsh weather and disaster conditions, and backup power sufficient to maintain operations for an extended period of time.

2.5.2 PSST Network Reliability, Availability, and Hardening Expectations

- (1.) Public Safety desires and has a need for the SWBN to be useful for mission critical communications during extremely adverse operational and weather conditions. The higher the level of communications reliability and availability, the more effective public safety can be at executing their jobs during the most critical times of need. The goal is to construct a highly reliable and available network that is better than commercial wireless networks today, yet economically viable. This can be achieved through many means such as hardening the terrestrial network, strategic storage staging and use of emergency deployable infrastructure and back up reliance on satellite coverage.
- (2.) As discussed above in Section 2.4.3(4)(a), the RF signal reliability is expected to be 95% over 95% of the area covered. The RF link is not included when calculating the infrastructure availability numbers that follow.
- (3.) The system is expected to provide 99.9% availability at Year One of operation calculated on jurisdictional boundaries. The exact method for measuring availability will be negotiated as part of the NSA; however, the intent is for this to be a measure of infrastructure availability as measured from the antenna back through the core network and will exclude scheduled maintenance downtime as coordinated with the PSST. In preliminary meetings with prospective bidders, multiple methodologies for calculating availability were identified and the PSST will solicit input from prospective bidders during upcoming meetings to further define this calculation.
- (4.) SWBN specifications must include attributes such as hardening of transmission facilities and antenna towers with backup power to maintain sufficient operations for an extended period of time as needed for weather and disaster conditions in a given area based on industry's best practices and local building codes, including, but not limited to, seismic safety standards, wind, ice and other natural phenomenon.

- (5.) The SWBN cellular-like network architecture obviates the need for economically non-viable reliability and availability measures such as any requirement for extended power and redundant backhaul at every site, such as might be the case (since the number of sites and the cost would be lower), with traditional public safety high-site, high-power systems. However, critical sites shall have battery backup power of 8 hours and generators with a 5 to 7 day fuel supply. Some percentage of sites will require redundant backhaul to meet the network availability standard. The D-Block winner and the PSST will work together with local public safety agencies to identify critical sites factoring in space, cost and other constraints that may impact hardening ability.
- (6.) The use of emergency deployable infrastructure, will be factored into the overall network availability.

2.6 Network Capacity

2.6.1 FCC Rule

§ 27.1305 (2)(d); § 90.1405 (2)(d)
Sufficient capacity to meet the needs of public safety.

Second R&O Para 405

Sufficient capacity to meet the needs of public safety, particularly during emergency and disaster situations, so that public safety applications are not degraded (*i.e.*, increase blockage rates and/or transmission times or reduced data speeds) during periods of heavy usage.

2.6.2 Network Capacity Expectations

- (1.) The SWBN must have sufficient capacity to meet identified needs of public safety, including but not limited to, during times of emergency.
- (2.) To help optimize the D Block operators planning for public safety and other Public Safety Users' usage on the SBWN, the PSST will provide a rolling 12-month usage forecast on a quarterly basis.

2.7 Network Security and Encryption

2.7.1 FCC Rule

§ 27.1305 (2)(e); § 90.1405 (2)(e)
Security and encryption consistent with state-of-the-art technologies.

2.7.2 PSST Network Security and Encryption Expectations

- (1.) The SWBN should implement controls to ensure that public safety priority and secure network access is limited to authorized public safety users and devices.
- (2.) The SWBN should utilize an open standard protocol for authentication.

- (3.) Some of public safety's unique needs are not provided for in a commercial service context. The SWBN should allow for public safety network authentication, authorization, automatic logoff, transmission secrecy and integrity, and audit control capabilities as well as other unique attributes that may be defined in the final negotiations.
- (4.) There should be a joint effort by the PSST and the D Block winner to introduce into commercial technology standards bodies the security and encryption and other functional specifications that are needed by public safety to effectively execute its mission and responsibilities.
- (5.) PSST recommendations for administrative safeguards and controls for security management, oversight, incident management, and privacy into the D Block winner's technical and operational parameters, as well as procedures should be incorporated.
- (6.) Compliance with FBI Criminal Justice Information System (CJIS) guidelines which include physical security guidelines, advanced authentication methods, unique identifiers for authenticated users. Standards for network security also will be complied with and incorporated.

2.8 Network Priority and Quality of Service (QoS)

2.8.1 FCC Rule

§ 27.1305 (2)(f); § 90.1405 (2)(f); § 27.1307

A mechanism to automatically prioritize public safety communications over commercial uses on a real-time basis consistent with the requirements of § 27.1307.

Second R&O Para 405

A mechanism to automatically prioritize public safety communications over commercial uses on a real-time basis and to assign the highest priority to communications involving safety of life and property and homeland security consistent with the expectations adopted in this Second Report and Order.

2.8.2 PSST Public Safety Priority and Quality of Service (QoS) Expectations

The technology deployed on the SWBN ultimately will determine the specific method used to provide network priority and QoS to meet the PSST's priority and QoS expectations.

Within all current advanced broadband technologies, varying levels of capabilities exist to provide degrees of priority and QoS management. Consistent with the FCC requirements, public safety and other PSST approved priority users will be assigned the highest level of network priority and QoS on the SWBN by the PSST.

2.8.3 Priority

- (1.) Priority will be defined as PSST-approved and assigned user, network, application, and services priorities that, via user and/or device identification, offer the highest assignable levels of priority for network access and use of network resources, services, and applications as defined and agreed to in the NSA.
- (2.) Public safety and other PSST approved priority users will be provided priority service that will allow for different levels of service priority, based on the given role of a user.
- (3.) The highest 50% of access priority levels available in the radio access network technology will be allocated for assignment and use only as public safety and other priority levels as approved by the PSST.
- (4.) In the event that the network bandwidth is not available or is congested due to commercial use, the network will provide a mechanism to accommodate public safety users by pre-empting commercial users who are operating on public safety's spectrum.
- (5.) The SWBN will provide an appropriate priority to 9-1-1 calls per applicable FCC requirements; 9-1-1 calls should not be subject to pre-emption.

2.8.4 Quality of Service (QoS)

- (1.) The determination of QoS classes is technology-dependent, but it is anticipated that the SWBN will support up to 7 defined classes of service.
- (2.) QoS will refer to resource reservation and session control mechanisms.
- (3.) QoS mechanisms will provide different levels of performance to a traffic/data flow in accordance with predefined class of service and its associated performance parameters for identified applications and/or services.
- (4.) QoS will be considered the full class of mechanisms that are found at multiple IP layers in the network (both RAN and Core) to provision and apply priority for IP packet based traffic.
- (5.) The assignment of network resources will take into account the user and/or service priority as well as the QoS requirements of the application.
- (6.) The SWBN will support multiple QoS flows between a user device and network, where each flow may have a different QoS requirement and priority level.
- (7.) If network resources are not available to meet a resource reservation request the SWBN should have the ability to negotiate a mutually acceptable QoS with the user device.
- (8.) All PSST priority user logical client-based VPN and layer 2/3 Virtual Private Network (VPN) will be configured and provisioned within the SWBN to have the highest authorized IP packet routing and queuing treatment.
- (9.) The methods by which QoS will be promulgated across the SWBN will be dependent on the technology employed. Therefore, the PSST expects that the D Block winner will partner with the PSST to identify and document the configuration parameters for the chosen SWBN technology required to provide the specified QoS for the PSST authorized or designated services, applications, and permissions.

2.9 Operational Capabilities - Network Services and Applications

2.9.1 FCC Rule

§ 27.1305 (2)(g); § 90.1405 (2)(g)

Operational capabilities consistent with features and requirements that are typical of current and evolving state-of-the-art public safety systems.

Second R&O Para 405

Operational capabilities consistent with features and expectations specified by the public safety broadband licensee that are typical of current and evolving state-of-the-art public safety systems (such as connection to the PSTN, push-to-talk, one-to-one and one-to-many communications, etc.).

2.9.2 Network Services and Applications Expectations

- (1.) Public safety should have access to the full suite of current and continually evolving commercial services and applications hosted on the SWBN.
- (2.) All approved PSST-hosted and/or other third party public safety applications and services will be delivered via the SWBN consistent with specified performance and network transport and routing parameters.
- (3.) There will be mechanisms for monitoring SWBN adherence and conformance to specified service quality and performance standards, including:
 - (a) Creation of service level agreements (SLA) and associated key performance indicator (KPI) definition, metrics, and reporting
 - (b) SLA conformance oversight and management
 - (c) SLA violation and shortfall identification, notification, and correction
- (4.) The D-Block winner should provide both services related SLA reports and access to the source data for such reports. The specific metrics, format, reporting intervals and other elements of performance oversight will be agreed to in the NSA.
- (5.) Reporting requirements for extraordinary, emergency, and incident events will be considered separate and distinct from the scheduled reporting and will be defined and agreed to within the NSA.
- (6.) Table 2.9.2-A provides an example list of applications and services that should be supported on the SWBN. The stated data rates are based on current application supplier specifications. Actual parameters such as delay, delay variation, throughput, etc, in addition to the stipulated KPI's for such applications and services, will be negotiated in the NSA.

Table 2.9.2-A

Application/Service	Description	Data Rate
File transfer	Download of such items as high-resolution images, GIS data, etc.	Greater than 256 kb/s
Email		Less than 16 kb/s
Web browsing		Greater than 32kb/s
Cellular voice	Analogous to CMRS Voice	4-25 kb/s
Push to talk voice	Analogous to CMRS PoC	4-25 kb/s
Indoor video	Video that is transmitted from inside a building / tactical or surveillance	20-384 kb/s
Outdoor video	Video that is transmitted from the street / tactical or surveillance	32-384 kb/s
Location services	This includes location services for personnel, vehicles and other objects	Less than 16kb/s
Database transactions	This includes both remote and local jurisdictional databases	Less than 32kb/s
Messaging	Instant messaging and SMS type services, both one-way and two-way.	Less than 16kb/s
Operations data	This is a catch all for data that deals with the operations and maintenance of the network, i.e. over the air programming, remote client management, etc.	Less than 32kb/s
Dispatch data	This area primarily covers data as it relates to computer aided dispatching.	Less than 64kb/s
Generic traffic	This is a catch all for traffic that doesn't fall within any of the categories described above, and that generates less than 64kb of data per second.	Less than 64kb/s
Telemetry	Remote measurement and reporting of information for radio devices, vehicles, etc. Also includes sensors data such as passive chemical detection. Additionally, biometric sensors that require better network performance are also included in this application class.	70-120 kb/s
Virtual Private Networking		Less than 64kb/s

2.10 Operational Control - Public Safety Command and Control

2.10.1 FCC Rule

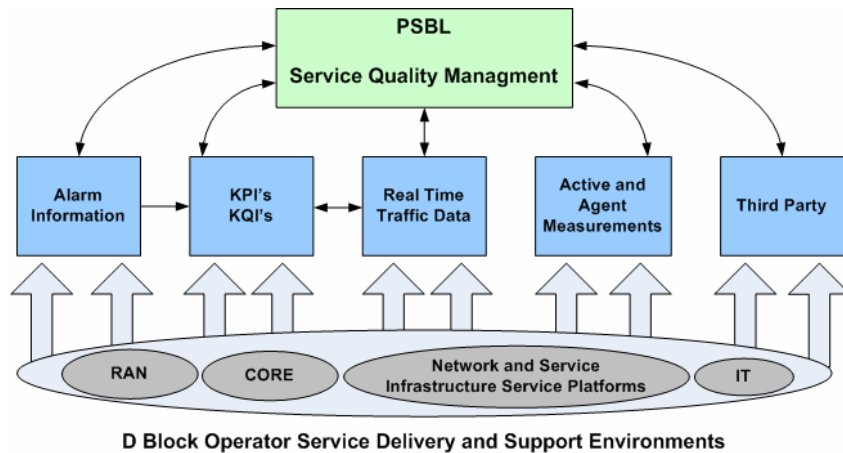
§ 27.1305 (2)(h); § 90.1405 (2)(h)

Operational control of the network by the public safety broadband licensee to the extent necessary to ensure that public safety expectations are met.

2.10.2 Local Public Safety Command and Control Expectations

- (1.) Real-time and near real-time SWBN OSS/NMS-based visibility to network and service quality status. The type, content, source, display, delivery format, security, reliability and other key design parameters will be addressed in the NSA.
- (2.) The ability by the PSST to manage and operate separate logical and/or physical databases (Home Location Register, Home Subscriber Server, Authentication, Authorization, & Accounting systems) of public safety user equipment provisioned for use on the SWBN in a format to be addressed in the NSA.
- (3.) The ability by the PSST to host services that may require elements of IP Multimedia Subsystem (IMS) or System Architecture Evolution (SAE) environments for the control and management of services.
- (4.) PSST and/or authorized public safety entities access, via service management applications with control to setup, modify user / user group / application priorities profiles, provision or add, manage, and authenticate users and devices.
- (5.) PSST and/or authorized entities will have access to an over-the-air management framework for managing public safety user devices (individually or in groups of devices) to clear user data or disable devices.
- (6.) The PSST must be informed of malfunctions or failures that impact end users' services and applications over a wide area. The time frame for such notifications, the format, and the scenarios in which this information is required will be addressed in the NSA.
- (7.) Notification to the PSST of system downtime (or any work that may affect service or system performance over a wide area) due to planned maintenance, configuration changes, or upgrades. The PSST will provide the D Block winner with advance notice periods to address planned public safety events. The PSST will coordinate with local public safety entities affected by these activities.
- (8.) Figure 2.10.2-A and the list of indicator examples set forth examples of the types of elements to be correlated to provide the level of information by which the PSST can offer oversight and service QoS to its priority users. This topic will be negotiated and included in the NSA.

Figure 2.10.2-A Service Quality Information Flows and Sources Example



Service Quality Management Indicator Examples:

- * Service Availability
- * Service Accessibility
- * Service Access Time
- * End to End Delay
- * Delay Variation (Jitter %)
- * Access Delay (Ntwk/Svc)
- * Release Failure
- * Continuity of Service Connections
- * Quality of Sessions
- * Average Bearer Bit Rate by Service Class
- * System Responsiveness (e.g. interactive)
- * One Way Transmission Delay
- * Payload Content Preservation
- * % Packet Mis-Direction Per Session

2.11 Public Safety Device Selection and Satellite Devices

2.11.1 FCC Rule

Second R&O Para 405

The Public Safety Broadband Licensee shall have the right to determine and approve the specifications of public safety equipment that is used on the network, and the right to purchase its own subscriber equipment from any vendor it chooses, to the extent such specifications and equipment are consistent with reasonable network control expectations established in the NSA.

A requirement, as explained more fully herein, that the Upper 700 MHz D Block licensee make available to the Public Safety Broadband Licensee at least one handset that would be suitable for public safety use and include an integrated satellite solution capable of operating both on the 700 MHz public safety spectrum and on satellite frequencies.

2.11.2 PSST Device Selection and Satellite Device Expectations

(1.) Device Selection

- (a) The right to determine and approve specifications and the right to purchase subscriber equipment from any vendor, provided that such specifications and equipment are consistent with the reasonable network control requirements established in the NSA.

(2.) Satellite Device

- (a) One handset that would be suitable for public safety use and an integrated satellite solution capable of operating both on the 700 MHz public safety spectrum and on satellite frequencies.
 - i. The PSST expects that this device would also work on the D Block spectrum.
 - ii. The PSST expects to work in conjunction with the D Block winner in selecting the satellite provider(s) in order to negotiate the best wholesale rate for satellite service.
 - iii. The PSST expects that this capability will be incorporated into the devices and SWBN no later than the fourth quarter of 2010.

3 PSST and D Block Winner Partnership Relationship

The PSST desires to “partner” in key areas with the successful D Block winner in the development and delivery of nationwide SWBN services to Public Safety Users. To this end the concept of the PSST as both the agent and licensee for Public Safety Users on the SWBN is outlined within Section 3.

3.1 PSST Ownership Position

- (1.) In light of its intended roles and responsibilities, the PSST expects to occupy a meaningful “ownership” position, giving it direct involvement with respect to all public safety and, subject to FCC approval, other PSST approved users such as Federal public safety (“Public Safety Users”) on the national SWBN.
- (2.) Accordingly, the PSST expects to “own the customer,” so that it will be in a position to:
 - (a) define and control the customer experience (by, *e.g.*, assigning or modifying priorities in real time),
 - (b) monitor and enforce its commercial network operator/partner’s compliance with applicable SLA’s and QoS standards to be set forth and identified in the NSA; and
 - (c) respond, rapidly and directly, to expressed needs for and with respect to all Public Safety Users on the SWBN.
- (3.) The PSST also expects that it may want or may need to, subject to NSA negotiations:
 - (a) operate certain items of network infrastructure equipment (*e.g.*, a separate NOC, HSS and AAA complex for Public Safety Users on the SWBN);
 - (b) provide or control the provision of certain network and related ancillary and support services to the SWBN’s Public Safety Users (*e.g.*, billing and care); and
 - (c) in certain cases, make available certain of such capabilities and related equipment to local Public Safety User organizations to enable them to play an active role in the delivery of wireless broadband communications and ancillary services to their own Public Safety Users.
- (4.) To accomplish and facilitate the above, the PSST may request in the NSA negotiations that the D Block commercial network operator/partner:
 - (a) permit the PSST to play the roles described above, if and to the extent the PSST chooses to do so; and

- (b) make all reasonable accommodations requested by the PSST to integrate, coordinate and/or harmonize the network operations, infrastructure and systems of the commercial network operator/partner with those of the PSST to assure the intended efficient operation of the SWBN and of any related “virtual Public Safety User network” that the PSST may define and create on it.

3.1.1 Background and Rationale for 3.1

The Second R&O contemplates that the PSST will have, as one of its core roles and responsibilities, the administration of access to the SWBN for users that should appropriately look to the PSST for that purpose. To effectively and reliably discharge this important responsibility in a way that will provide certainty both to the PSST and to those users on the SWBN whose interests the PSST is charged with representing and advancing, the PSST believes that it will need to be actively involved in the processes of delivering services, applications, and access devices to SWBN users that are entitled to receive: (a) the highest service priority assignments, and (b) the ability to pre-empt other users on its spectrum, to the extent required to assure those Public Safety Users “as needed” emergency access to the SWBN and to appropriate service quality in line with the relevant SLA and other QoS standards that will be set forth in detail in the NSA and related documents.

3.2 PSST Rights to “Priority Services” and Public Safety Users

- (1.) To assure orderly and efficient operation of the SWBN, the PSST believes that it should have exclusive rights to provide “priority services” to Public Safety Users on the SWBN.
- (2.) It is understood that the commercial network operator/partner would retain the rights (directly or through its commercial agents, partners or affiliates, or to or through third party resellers or wholesale customers, to the extent permitted by FCC rules and regulations and the terms of the NSA) to make available, offer and provide commercial services on the SWBN (including services that may be assigned priority levels that are lower than those reserved for Public Safety Users on the SWBN), and/or related user devices for such purposes, to any potential users (including any individuals who would qualify as potential Public Safety Users, but who conclude that normal, commercial services – on the SWBN or elsewhere – adequately meet their needs and requirements).

3.2.1 Background & Rationale for 3.2

Although the Second R&O contemplates that the PSST will be afforded significant flexibility and control in connection with the construction and use of the SWBN, the PSST believes that its exercise of such flexibility and control is best circumscribed and limited within well defined and logically drawn domains, both from a user and a service standpoint. However, within those domains, the ability of the PSST to exercise that flexibility and control, as it deems in the best interests of those users whose interests the PSST is properly charged to protect and promote, should be paramount. Conversely, the PSST’s commercial network operator/partner should enjoy a comparable degree of autonomy, control and flexibility when it is operating in the areas of its traditional and appropriate business focus.

The PSST believes that orderly and efficient operation of the SWBN can best be assured, for the benefit of both the Public Safety Users and the normal commercial subscribers on the SWBN, if the PSST brings a dedicated and exclusive focus to the provision of “priority services” to the Public Safety Users on the SWBN, and if its commercial network operator/partner retains exclusive rights to provide normal commercial services to all users on the SWBN, consistent with the appropriate focus and specialized expertise of a commercial wireless services provider. The PSST believes that having two different parties simultaneously responsible for the same (or overlapping) areas of network operation would, at a minimum, be expected to make coordination or dovetailing of the parallel activities difficult at best, and could lead to chaos. That would be especially true when the added pressures of an emergency response situation enter the picture. Equally debilitating would be a “common and co-equal” responsibility with respect to focus on and responsibility for particular network services and customer groups.

A commercial network operator can be expected to have considerable experience in providing normal, commercial grade wireless services (which may include the assignment of priorities, at levels below those reserved for assignment by the PSST to the Public Safety Users on the SWBN, to commercial subscribers and/or their commercial grade services) to mainstream customers who determine that level of service is reasonably appropriate to their needs. Such mainstream customers could include individuals whose occupational category and/or responsibilities would qualify them as potential Public Safety Users entitled to receive “priority services” on the SWBN, but who elect to subscribe for normal, commercial grade wireless services provided by a commercial network operator. By contrast, the PSST is charged with the overall authority for crafting the SWBN so that it will be as responsive to the legitimate requirements of Public Safety Users as valid commercial considerations will reasonably permit, and this responsibility encompasses not only the construction, but also the use, of the SWBN. Given that objective, the PSST believes that a division of responsibility between it and its commercial network operator/partner, for “priority service” delivery to Public Safety Users who elect it, and normal commercial service delivery to all users who elect it, respectively, is a sensible one that the PSST intends to request.

3.3 PSST Management of Public Safety User Access Rights and Privileges

- (1.) The PSST expects that it will be the sole assigner/remover/modifier of those “priority access rights” that will be reserved for Public Safety Users on the SWBN. Subject to temporary or emergency grants of “priority access rights” with the express consent of the PSST (in accordance with terms to be specifically delineated and included in the NSA), no user should have those special “priority access rights” on the SWBN unless the user received those rights by also obtaining “priority services” and related user devices for such purpose from the PSST or a source authorized for those purposes by the PSST.
- (2.) **Definitions of Certain Terms:** For purposes of the above,
 - (a) *priority services* means the provision of communications services to a particular user on the SWBN:
 - i. in such a manner that those services are superior, in one or more material respects (e.g., in terms of their use of network resources,

- or possession of quality or performance attributes), to the same or the most nearly comparable type of communications services that are then provided to at least one other definable and distinct group of users on the SWBN (such other group or groups, “lower priority users”); and
 - ii. that are identified by a priority level or levels (to be specified in the NSA) that will be reserved for assignment by the PSST to Public Safety Users on the SWBN; and
 - iii. where the availability and/ or delivery of such communications services to that same user on the SWBN can be guaranteed or enforced by automatic, real-time delay or degradation of quality (or, to the extent required, termination) of communications services (such termination, delay and/or degradation, “service pre-emption”) then being provided to lower priority users on the SWBN, to the extent such service pre-emption is then required to enable the desired communications services to be provided to that same user on the SWBN .
- (b) *priority access rights* means those access rights granted to a particular user on the SWBN (e.g., rights to access control channels, or to access network capacity and resources) to the extent required or necessary for the provision of *priority services* to that same user on the SWBN.

3.3.1 Background & Rationale for 3.3

For substantially the same reasons as set forth in 3.1 and 3.2 above, there should be only a single process for obtaining, removing or modifying the special “priority access rights” of Public Safety Users on the SWBN, and a single party should be in ultimate control of that process. Any other approach could introduce needless risks of confusion, inconsistency and unpredictability into these crucial areas of administering access to the SWBN, to the detriment of those for whom the smooth, predictable and reliable performance of the SWBN is the most critical – the Public Safety Users and the members of the public who are relying on them in a natural disaster or other emergency situation. The ability of the commercial operator to determine to assign lower levels of priority to particular commercial subscribers and/or to particular commercial grade services on the SWBN is not intended to be precluded or otherwise limited by the existence or implementation of the special “above commercial” priority access rights or priority services that are assignable by the PSST to Public Safety Users on the SWBN.

3.4 PSST SWBN Wholesale Rates

- (1.) If the PSST designs, creates and operates a “virtual Public Safety User network” on the SWBN, the PSST would expect to buy minutes and bits produced on the SWBN at a discount to the then prevailing commercial rates for the most closely corresponding service offering. Such an outcome could be achieved in a variety of ways, for instance, through reliance on negotiated, formula-determined rates (wholesale or retail, as appropriate to the circumstances) that could be specified in the NSA or through a negotiated percentage discount from prevailing commercial service offering reference rates (wholesale or retail, as appropriate).

- (2.) The PSST would expect to consider a number of factors in selecting a rate-setting approach for inclusion in the NSA, including, most significantly, the following:
- i. the FCC's reasoning, expressed in the Second R & O, that the negotiated usage fees should not include any elements designed to allocate among or recover from public safety users any significant items of capital or other costs associated with the initial build of the SWBN;
 - ii. the legitimate expectations of the commercial network operator/partner to , recover, through usage rates, identified and averaged "operating costs" incurred by the commercial network operator/partner in providing or making available services on (or in connection with) the SWBN to Public Safety Users and, where relevant, to the other users on the SWBN .
- (3.) The central purpose behind these concepts is twofold:
- (a) The PSST believes that it is appropriate both to assure that the commercial network operator/partner designed (at minimum) to recover its operating costs while also assuring that such cost recovery from Public Safety Users on the SWBN would be limited to those categories of operating expenses that are clearly identified with services actually provided on the SWBN to Public Safety Users. As an example, if, as the PSST anticipates, it would "own" the Public Safety Users, in the sense of arranging for their SWBN service, supplying their user devices for that purpose, and providing related support services, such as provisioning, care, billing and collections, it would be inappropriate for those users' rates to incorporate charges designed to recover marketing and other customer procurement expenses (including device subsidy amounts). Likewise, in such circumstances, support system costs and personnel expenses incurred by the commercial network operator/partner, but associated with services provided to the commercial subscribers on the SWBN, would be inappropriate to be incorporated as part of Public Safety User rates. Of course, if the PSST were to elect to source certain services or functions for the benefit of the Public Safety Users on the SWBN through its commercial network operator/partner, then it would be appropriate to include the related expenses in the negotiated rate structure.
 - (b) Such an approach also is designed to provide the Public Safety Users on the SWBN with the intended economy of scale benefits derived from the Public/Private partnership, shared network arrangements. By assuring that the relevant categories of operating costs will be spread across all users of the SWBN (regular commercial subscribers as well as Public Safety Users) on an "averaged costs" basis, generally in proportion to their actual consumption of minutes and bits during the relevant period. This approach explicitly rejects the concept that certain identified costs – presumably, those associated with network attributes or features that were "requested by or designed specifically for public safety" – should be allocated exclusively to Public Safety Users. The PSST believes such an outcome would be inappropriate on several grounds. Most notably, it would effectively eliminate a large portion of the "economy of scale" benefits associated with the Public/Private partnership, shared network arrangements. More importantly,

- it ignores the practical reality that *all* network users *can* benefit from many network attributes and features regardless which type of user requested them or for whom they were designed – including features like the SWBN's enhanced coverage footprint, its higher levels of reliability and redundancy, and its adherence to higher SLA standards. Of course, it may be the case as well that certain network services or features could be available only to Public Safety Users and could have associated costs to the commercial network operator/partner – a possible example could be the use of governmentally mandated encryption protocols for certain Public safety user communications on the SWBN – in which case it would be entirely appropriate to impose the related cost recovery obligation on the relevant Public Safety Users, and to exclude any recovery of those costs from the rates imposed on normal commercial users on the SWBN.
- (4.) Finally, the PSST would expect that the negotiated rate structure – whether determined through a formula-based approach, through an approach involving discounting appropriate commercial reference rates, or through some other approach agreed by the parties and included in the NSA – would include (explicitly or implicitly) a to-be-agreed profit margin for the commercial network operator/partner, with the amount of that margin determined in the light of all relevant factors, including the nature and extent of the activities being provided by that operator/partner to the PSST and the Public Safety Users on the SWBN, the nature and extent of the risks involved in those activities, and similar factors usually influencing rates of return.
- (5.) Consistent with the above, the PSST expects that it would be permitted to purchase minutes and bits, meeting applicable SLA and other QoS and performance requirements, from its commercial network operator/partner at negotiated wholesale rates (or, if the PSST opts to follow a service approach involving the sourcing from its commercial network operator/partner of many of the ancillary services normally associated with a typical “retail subscriber” type arrangement, to have the related rates for such services established on a uniform, nationwide “pooled single account” purchase basis, such as would be the case for a large enterprise customer of a commercial network operator). However the parties determine to approach and resolve the rate setting tasks in their NSA negotiations, the PSST expects that the final agreement and outcome on these topics would be consistent with the objectives of:
- (a) establishing a “preferred rate structure” for the PSST in its dealings with its commercial network operator/partner that would lead to the “lower than typical commercial rates for analogous services” result contemplated in the Second R & O; and
 - (b) providing a reasonable degree of assurance that the operator/partner could expect to make a return – on an actual cost of services provided basis – by providing “minutes and bits” and possibly other services for the Public Safety Users on the SWBN.

Moreover, the PSST also expects that any basic agreement on rate setting that the parties incorporate in the NSA would have certain limitations and, like most general rules, likely would be subject to certain exceptions. Those exceptions would be developed and defined during the course of negotiating the NSA to address special circumstances or situations like those outlined below.

- (6.) During the early years of the SWBN's operation, any approach based on or otherwise designed to achieve actual operating cost recovery cannot be expected to work well for any users – whether commercial subscribers or Public Safety Users – if it is applied in a literal fashion, because the requisite cost scaling would not yet have occurred, and averaging total costs over actual users would produce absurdly high per user charges. So, at minimum, the PSST expects that the NSA would contemplate that some derived “normalized” average cost structure would have to be used as a reference point during this start up/ scale up phase of the SWBN.
- (7.) As a practical matter, given business realities, there will need to be some level of aggregate SWBN capacity usage by Public Safety Users that the PSST and its commercial network operator/partner will need to agree to – and perhaps to agree to shifts in that level over time – as the maximum capacity that can be purchased by the PSST pursuant to “discounted pricing” approaches such as the ones described above. This statement simply recognizes the fact that there are levels above which usage by Public Safety Users of the SWBN's capacity – regardless how legitimate and appropriate that usage is – will impinge unreasonably on the commercial network operator/partner's ability to earn a normal commercial return by providing service on the SWBN to its commercial subscribers, a result which could threaten the viability of its business and, therefore, the SWBN itself. If and when that “line” is crossed, it should be appropriate for a different pricing model or approach – one having as its main objective to make the commercial network operator/partner indifferent between providing such “excess use” to Public Safety Users and providing normal commercial services to its commercial subscribers on the SWBN – *i.e.*, to equal the “yield” (adjusted for any reduction in cost associated with serving Public Safety Users at wholesale instead of commercial users at retail) that the commercial network operator/partner would have expected to achieve had those minutes/bits been sold to commercial users.
- (8.) As a final example, any “discounted pricing” approach should de-couple (except in the cases noted above, and any other similar exceptions that may be agreed to in the NSA) the negotiated price of the minutes/bits purchased and the quantity purchased (except as the actual operating cost structure of the SWBN is influenced by the overall quantity of minutes and bits generated for all users during the relevant period). The PSST believes that the normal “quantity buy” approach (whether at wholesale or at retail) in the wireless context, which would have “use it or lose it” features associated with a specified quantity buy, a “premium pricing” penalty for usage over the specified quantity, and an option to meet or not meet the excess demand would be wholly inappropriate here for a variety of reasons. First, it will be impossible to predict, or even to project, with

certainly aggregate minute/bit demand by the SWBN's Public Safety Users – the very thought of doing so makes about as much sense as asking a fire company how many gallons of water they expect to need next month and expecting to receive an accurate answer. Second, in the event the PSST were to commit to buy more minutes/bits than it turns out the Public Safety Users on the SWBN actually need, it will not be possible (on the assumptions that the PSST will restrict its focus to providing only “priority services”, and then only to Public Safety Users, on the SWBN) for the PSST realistically to “dump” its excess minute and bit inventory by discounting prices. Finally, and most significantly, the ultimate Public Safety Users that are expecting to receive “priority services” on the SWBN cannot realistically have their service “cut off” when the assumed aggregate minute/bit demand is reached, and if “excess supply” were available for purchase only at premium prices, the ability of those users to absorb what could be significant (and, by definition, unforeseen and unbudgeted) costs could jeopardize their continuing effectiveness. Of course, the PSST would consider it appropriate to obligate the PSST and the affected Public Safety Users to take reasonable steps, such as requesting any emergency communications expense reimbursement funds that may be available from governmental sources in declared disaster or emergency situations, and providing some of the amounts actually received to the commercial network operator/partner as additional compensation for any extra costs it may incur in such scenarios when Public Safety User demand unexpectedly spikes on the SWBN.

3.4.1 Background & Rationale for 3.4

The Second R&O envisions that Public Safety Users on the SWBN will be assessed reasonable rates for their network usage, and proceeds to outline guidance as to certain factors that should influence the negotiation of those rates and the ultimate result intended to be achieved. Specifically, the FCC highlighted its belief that, although typical commercial rates for analogous services may be a useful guide in the negotiations process, the negotiated rates would, in fact, be lower. The FCC cited several reasons that would lead to such a conclusion, including its expectation that the usage fees would not be set to recover any appreciable portion of the initial construction costs of the SWBN and that the negotiated fee terms would best serve the public interest goals outlined in the Second R&O, including ensuring that Public Safety Users of the SWBN are able to afford the “priority services” they require for their public safety functions.

In view of that guidance, the PSST has reached several preliminary conclusions regarding the approach it intends to pursue in the negotiation of fees for the “priority services” that are provided to Public Safety Users on the SWBN. Although this topic holds the potential to be among the more contentious aspects of the overall NSA negotiation process, the PSST is hopeful that, by advancing its preliminary thinking and reasoning prior to the commencement of the D Block auction, potential bidders can make their decisions regarding participation in the D Block auction on a more informed basis. The PSST does not mean to convey that it is wedded to any particular approach or methodology on this topic, as attaining a satisfactory outcome ultimately will be far more important than the means employed to achieve it.

3.5 Spectrum Lease Payment

- a. The PSST intends to request the D Block winner to make a cash payment of specified size to the PSST upon the signing of the NSA, which would serve as the first year's spectrum lease rights rental payment. Thereafter, for a specified number of years, an annual fixed amount payment (which the PSST would presume to be the same as the amount of the initial payment) would be due from the D Block winner to the PSST, representing the annual spectrum lease rights rental payment for each year.

3.5.1 Background & Rationale for 3.5

The Second R&O mandates a long-term spectrum manager leasing arrangement pursuant to which the D Block winner will be granted certain pre-emptible secondary usage rights to the 10 MHz of public safety broadband spectrum that is (expected to be) licensed to the PSST. In these circumstances, the PSST believes that it is appropriate to request a lease payment – to be made annually – from the D Block winner to reflect the value potential inherent in the spectrum usage rights that would be granted under that lease. Such a lease payment, in part, recognizes that compensation to the licensee would be a normal attribute of such spectrum usage arrangements, and, in part recognizes the unavoidable fact that the PSST will need an assured source of funding, especially to reimburse its own start up expenses, expenses it expects to incur before and during the NSA negotiations and during the construction phase and the early start-up/scale up period of the SWBN, when any Public Safety User operations on the SWBN – and related usage fees – can be assumed to be either entirely absent or an inadequate source of free cash flow to supply the funding that the PSST will require to effectively discharge its obligations. Additionally, any Public Safety User operations that the PSST may define and create on the SWBN will require some form of financing – whether to fund necessary capital expenditures, to finance operating losses during the start up/scale up period of those operations or to serve as a source of working capital. Although some of the funds needed for those purposes may be available from private investors, the PSST's need to retain meaningful control over those activities necessitates that it have access to a known, predictable source of cash for some period of time that could be tapped as a potential source of its share of the financing for those purposes, if it chooses to do so.

The PSST recognizes that the economics associated with the Public/Private partnership structure and shared network arrangements will be complex and will involve many interdependencies. Nonetheless, the PSST thinks that it is reasonable to expect that the ability to make commercial usage of public safety spectrum – having a uniform, nationwide footprint - should carry a value, and that value can best be captured through the mechanism of an annual spectrum lease payment. The amount of that payment may, in turn, depend on a variety of factors, including the amount of the winning bid for the D Block spectrum, the amount of the winning bids for other 700 MHz spectrum allocations, prices paid for 700 MHz spectrum in open market transactions, the portion of the capacity that could properly be viewed as associated with the public safety 10 MHz of broadband spectrum that would be presumptively devoted – on average – to meeting Public Safety User demands on the SWBN and so would be unavailable for commercial use, the amount of incremental costs – above reasonable standard commercial network cost

expectations – that would be associated with complying with the commercial network partner/operator’s obligations under the NSA, the actual and reasonably estimable value to the commercial network operator/partner associated with the unique features of the SWBN, and the general economic and interest rate environment and other matters.

3.6 Coincident Market Launch of Commercial and Priority Services

- (1.) The PSST expects that the NSA will include a general rule (subject to appropriate exceptions) that no launch of commercial services on the SWBN can occur in any market if “priority services” could not then also be launched on the SWBN in that same market.

3.6.1 Background & Rationale for 3.6

The PSST believes that the general rule for launching markets on the SWBN should be that no commercial service launch should be permitted in any market if “priority services” could not then also be launched in that same market. A core element of the logic that supports the Public/Private partnership concept for the construction and operation of the SWBN is the assumption that activities will be oriented to satisfying the reasonable needs and expectations of each of the “partners.”

Although it hopefully will not be necessary to compel adherence to such a principle, the PSST believes that it would be prudent to request that the NSA contain provisions designed to guard against a mis-alignment of interests, away from serving the common good and toward ignoring or deferring the needs of the party least actively involved in the construction and operation of the SWBN – the PSST - and, derivatively, the Public Safety Users of the SWBN that it represents.

A mechanism of this type should provide additional incentive to the commercial network partner/operator, and additional assurance to the PSST and the Public Safety Users’ community in the affected market, that the SWBN’s “priority service” criteria and features (in terms of network coverage, reliability, hardness and redundancy, as well as availability of infrastructure, other systems and software and handsets to support the desired and agreed “priority” services complement as contemplated in the NSA) will be satisfied, available and functional in each market from the outset.

The PSST recognizes that there may be valid and logical reasons why “priority service” might not be ready for launch in a particular market at the same time as the initial commercial launch, and that there may be numerous circumstances in which the commercial network operator/partner has done all that reasonably could be required of it, and any “priority service” launch inability or delay could well be the fault of the PSST. These and similar matters should be addressed, and appropriate exceptions should be crafted, in the NSA.

3.7 PSST Device/Service Expeditious Testing and Approval

- (1.) The PSST intends to request that “open access” rules and streamlined processes (for pre-network use testing/approval) for Public Safety User devices and applications on the SWBN be included and clearly spelled out in the NSA.

3.7.1 Background & Rationale for 3.7

Although the Second R&O contemplates that the PSST will have the authority and responsibility to select and approve public safety user devices and applications, the FCC sensibly required that selection and approval process to occur in consultation with the commercial network operator/partner. The commercial network operator/partner undeniably will have a legitimate interest in verifying that devices and applications proposed to be placed on the SWBN will not damage it or adversely impact its intended functioning for all users, yet that interest is no more legitimate than the PSST's interest in assuring that devices and applications that would not damage or adversely impact the functioning of the SWBN are made available promptly to the Public Safety Users that would benefit from access to them.

Accordingly, the PSST intends to propose that the NSA contain provisions that would obligate its commercial network operator/partner to swiftly and diligently conduct and conclude its review and testing of any new devices and applications that are proposed for use by Public Safety Users on the SWBN, and to impose on that review and testing process accelerated time frames and meaningful reasonableness criteria designed to assure "no harm/no adverse effect" open access standards will apply to such devices and applications.

3.8 PSST Economies of Scale

- (1.) The PSST intends to request that the NSA include provisions requiring its commercial network operator/partner to obtain "pass-through deals and economics" arrangements from its 700 MHz goods and services providers and suppliers for the benefit of the PSST and/or local public safety organizations, and for use by the Public Safety Users on the SWBN.

3.8.1 Background & Rationale for 3.8

One of the main "economy of scale" benefits that Public Safety Users can derive from the Public/Private partnership structure is the ability to combine purchasing power and negotiation advantage with a commercial network operator and its customer base.

So-called "pass-through" arrangements, which are designed to extend the same terms, conditions and pricing (thereby effectively aggregating purchases by or for the PSST and/or local Public Safety User organizations with those of the commercial network operator/partner), can be one of the ways to accomplish that objective.

As examples, a separate Public Safety User NOC could be sourced from the same manufacturer as the one supplying the NOCs for commercial use on the SWBN on as favorable terms, conditions and pricing as if it had been bought by or for the commercial network operator/partner. The same would hold true for any servers, systems and other network-related hardware owned or operated by the PSST or its designees for the Public Safety Users of the network.

To the extent that modifications are required to goods or services to make them appropriate for Public Safety User purposes, there could be a related requirement that any additional work would have to be done by suppliers on "fair and reasonable terms," including rates identical to those applied to any customization or modification tasks

performed by the supplier of the relevant good or service for the commercial network operator/ partner.

So, for instance, if the PSST wished to use the same core billing platform for the SWBN's Public Safety Users, but needed special modifications made to the rating engines or the billing format, or wanted to use the same outsource provider of customer care services, but desired a dedicated group of service center employees trained consistent with a more demanding Public Safety User Service Level Agreement profile, the basic service cost pass-through should reflect equivalent treatment to the PSST, with add-ons or special modifications performed under a "fair and reasonable" charge schedule.

3.9 Satellite Services and Devices

- (1.) The PSST intends to pick satellite service(s) for Public Safety Users on the SWBN and the hybrid device development activity should be coordinated with that provider.
- (2.) The PSST believes that the most sensible and effective approach will first involve the selection by the PSST of the satellite services provider(s), after which the D Block winner will be required to make at least one satellite-capable hybrid handset/device available to the PSST for public safety use on the selected satellite network(s).

4 Appendix A Glossary / Acronyms

AAA	Authentication, Authorization and Accounting; where Authentication refers to the confirmation that a user who is requesting services is a valid user of the network services requested, Authorization refers to the granting of specific types of service (including "no service") to a user, based on their authentication, what services they are requesting, and Accounting refers to the tracking of the consumption of network resources by users.
BSC	The Base Station Controller (BSC) provides, classically, the intelligence behind the BTSs. Typically a BSC has 10s or even 100s of BTSs under its control. The BSC handles allocation of radio channels, receives measurements from the mobile phones, controls handovers from BTS to BTS (except in the case of an inter-BSC handover in which case control is in part the responsibility of the Anchor MSC).
BTS	The Base Transceiver Station, or BTS, contains the equipment for transmitting and receiving of radio signals (transceivers), antennas, and equipment for encrypting and decrypting communications with the Base Station Controller (BSC). Typically a BTS for anything other than a picocell will have several transceivers (TRXs) which allow it to serve several different frequencies and different sectors of the cell (in the case of sectorized base stations).
Core Network	3G & 4G mobile radio systems consist of two parts. The radio access network (RAN) and the CORE network. The core network is all elements other than the BTS that comprise a modern mobile network
GGSN	Gateway GPRS Support Node (GGSN) is network node that acts as a gateway between a GPRS wireless data network and other networks such as the Internet or private networks.
HLR	The "Home Location Register" is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network.
HSS	The "Home Subscriber Server" is the 3G & 4G equivalent of the HLR and is a database of subscriber data required to deliver services across the mobile network
IMS	The IP Multimedia Subsystem (IMS) is an architectural framework for delivering internet protocol (IP) multimedia to mobile users. It was originally designed by the wireless standards body 3rd Generation Partnership Project (3GPP), and is part of the vision for evolving mobile networks beyond GSM. Its original formulation (3GPP R5) represented an approach to delivering "Internet services" over GPRS. This vision was later updated by 3GPP, 3GPP2 and TISPAN by requiring support of networks other than GPRS, such as Wireless LAN, CDMA2000 and fixed line.

IP	The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched inter-network. IP is a network layer protocol in the Internet protocol suite and is encapsulated in a data link layer protocol (e.g., Ethernet). As a lower layer protocol, IP provides the service of communicable unique global addressing amongst computers.
NMS	Network Management systems- A Network Management System (NMS) is a combination of hardware and software used to monitor and administer a network.
NOC	Network Operations Center.
NSA	Network Sharing Agreement between the DBL and PSBL in accordance with FCC 07-132.
OSS	Operations Support Systems- the systems which are used to manage the telecom network itself, supporting processes such as maintaining network inventory, provisioning services, configuring network components, and managing faults. May include some components of the Business Support Systems (BSS) which manages customers, supporting processes such as taking orders, processing bills, and collecting payments.
PDSN	The Packet Data Serving Node, or PDSN, is a component of a CDMA2000 mobile network. It acts as the connection point between the Radio Access and IP networks. This component is responsible for managing PPP sessions between the mobile provider's core IP network and the mobile station (read mobile phone). It is similar in function to the GGSN (GPRS Gateway Support Node) that is found in GSM and UMTS networks
PSST	Public Safety Spectrum Trust: entity which has submitted an application to the FCC to be named the licensee for the 700 MHz Public Safety Broadband License
Public Safety Broadband Licensee	Public Safety Broadband Licensee: the entity chosen by the FCC as the licensee for the 700 MHz broadband public safety spectrum allocation with the authority to set the requirements for the 700 MHz Broadband Network.
RAN	A Radio Access Network (RAN) typically consists of Node B/Base Station Transceiver, Backhaul, Base Station Antennas, and an RNC/BSC/SAE
RNC	The Radio Network Controller (or RNC) is the governing element in the UMTS radio access network (UTRAN) responsible for control of the Node-Bs, that is to say the base stations which are connected to the controller. The RNC carries out radio resource management, some of the mobility management functions and is the point where encryption is done before user data is sent to and from the mobile. The RNC connects to the Circuit Switched Core Network through Media Gateway (MGW) and to the SGSN (Serving GPRS Support Node) in the Packet Switched Core Network.
SAE	System Architecture Evolution is the core network architecture of 3GPP's future LTE wireless communication standard. (note that this is provided as an example and does not suggest a RAN technology endorsement)

SGSN	A Serving GPRS Support Node (SGSN) is responsible for the delivery of data packets from and to the mobile stations within its geographical service area. Its tasks include packet routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles (e.g., IMSI, address(es) used in the packet data network) of all GPRS users registered with this SGSN.
Support Systems	Radio base stations, BTS node aggregation routers, RNC, IP gateways, operator HLR & AAA, operator Core Network, IMS/SAE systems, application services, and operation support systems and network management systems
SWBN	Shared Wireless Broadband Network
Transmission	Wired, wireless, or fiber communication transport links
VPN	A virtual private network (VPN) is a communications network tunneled through another network, and dedicated as a specific network in routing topologies.