Public Safety

700MHz Broadband

Statement of Requirements

Version 0.5

October 26th, 2007

Table of Contents

1 Scope

This document has been created to facilitate the dialogue between the Public Safety Broadband Licensee (PSBL) and the D-Block Licensee (DBL). It is intended to help potential D-block bidders make a participatory decision as to the auction and provide the foundation for the Network Sharing Agreement between the PSBL and DBL.

1.1 Change Log

Version	Date	Changes
0.1	October 22nd	This was the first complete draft created for vetting by the NPSTC Broadband Working Group.
0.5	October 26th	This is the draft that will go out for public safety review.

1.2 Acknowledgements

The National Public Safety Telecommunications Council Broadband Working Group would like to thank the many public safety practitioners, individuals, industry representatives, and government organizations that directly contributed to the creation of the Public Safety 700MHz Broadband Statement of Requirements.

1.3 Contact Information

Please address comments or questions to: NPSTC Broadband Working Group

700SOR@NPSTC.ORG

2 Intended Audience

This document is intended for two primary audiences: public safety and potential D-block bidders.

3 Operational Requirements

Section 3 Requirement #	Requirement Description	Additional Information
1	The DBL shall provide the PSBL (or its designated entity) a 24-hour, 7 days-a-week support for fixed and user equipment. The DBL will not be responsible for user equipment procured independently by individual agencies (with the exception of any warranties provided by DBL)	
2	In all cases, 24x7x365 access to call center support for issue resolution and assistance will be required.	

3.1 Access and Control

Section 3.1 Requirement #	Requirement Description	Additional Information
1	The DBL shall enable the PSBL to perform annual cell site, network, data center, and administrative facility spot audits to verify compliance to agreed to levels of hardening and emergency preparedness	
2	The DBL shall provide the ability to allow the PSBL (or its designated entity) to manage and operate a separate logical database of public safety user equipment provisioned to use the system.	
3	The DBL will provide real time access support to the PSBL and local public safety entities in line with jurisdictional boundaries to its provisioning and fulfillment services, with appropriate level of control over application flows and priorities, within a flexible framework to accommodate critical situations and incident response in addition to routine account and policy management. This includes but is not limited to: control, setup, modify user / user group / application priorities profiles, provision/add, manage, and authenticate users and devices.	
4	The PSBL requires that the DBL make accessible management and control interfaces for any end user services which it may provide to the public safety community.	

5	The DBL provides an over-the-air management framework to PSBL and/or local public safety for managing public safety user devices. This includes the ability to remotely upgrade operating software, software clients, clear user data, and to disable the device.	
6	The DBL shall provide the PSBL (or a designated entity) permission and capability to oversee the system operation.	
7	The DBL shall inform the PSBL (or a designated entity) of any malfunction or partial failures that impact service.	

3.1.1 Notification and Informational

Section 3.1.1 Requirement #	Requirement Description	Additional Information
1	The Public Safety Broadband Licensee and local public safety will require advanced notification of system downtime (or any work that may affect service or system performance) due to planned maintenance, configuration changes, or upgrades. PSBL must be able to coordinate maintenance windows with the DBL. PSBL can also specify exclusion time periods to address major public safety events (planned).	
2	The DBL shall provide coverage data and information quarterly, in a standard format and package this information for the PSBL to distribute to its users as necessary.	
4	The DBL shall provide the PSBL (or its designated entity) reports highlighting traffic per public safety user or device such as minutes of use and overall data usage. Reports such as Call Detail Records (CDR) or IP Detail Records (IPDR) shall be part of these reports.	
6	The DBL shall provide the state/local agencies access to record public safety application/service sessions.	This may include future CALEA support.
7	The network shall have a means to collect metrics (operational measurements) associated with the network's performance. The network shall be able to collect statistical data and export such data to an external server. Performance impacts due to such collection of data should be minimal.	

8	For failure analysis the PSBL requires the DBL ensure that all platforms produce availability metrics and the network includes intelligence to do event correlation as needed in order to compile reports detailing outages impacting Public Safety users' transactions.	
9	The PSBL requires the DBL ensure services provided to Public Safety users are instrumented to report performance metrics both to call processing and OSS infrastructure to guarantee specific performance levels as determined in the service level agreement (SLA).	
10	The PSBL requires the DBL provide mechanisms capable of aggregating performance statistics from network elements, with watermarks for typical Public Safety use and forecasted critical incident use based on modeling so that overbuild can be estimated in determining overall capacity requirements.	

3.1.2 General Hardening

3.1.2.1 Guidance

For disaster recovery and general hardening the PSBL suggest that each cell site and communications center be built to withstand extended power outages. The guidelines below are potential solutions that can provide a set of cell site build standards that would provide adequate support for public safety operations in power outage situations caused by some form of failure or disaster.

Section 3.1.2.1 Guidance #	**Guidance Description**	**Additional Information**
1	The PSBL and the DBL shall agree on a minimum of 4 levels of mobile cell site service priority levels. PL-1A Primary emergency and disaster response facilities PL-1B Secondary emergency and disaster response facilities PL-2 Targeted Critical infrastructure facilities, staging, or rally locations required for emergency and disaster PL-3 All other sites	Final definitions, requirements, attributes, configurations, target emergency or extraordinary stand-alone operating time frames for each level of classification shall be agreed to as part of the NSA process.

2	PL-1A sites shall have: 8 hours battery backup power Permanent Generators with 5 day fuel supply Fully Redundant Backhaul Transmission	
3	PL-1B sites shall have: 8 hours battery backup power Permanent Generators with 3 day fuel supply Emergency Microwave or other redundant backhaul transmission	
4	PL-2 sites shall have: 8 hours battery backup power Portable Generators with 1 day fuel supply Emergency Microwave or other redundant backhaul transmission	
5	PL-3 sites shall have: 8 hours battery backup power Standardized Connection To Portable Generator Emergency Microwave or other redundant backhaul transmission	

3.1.2.2 Hardening Requirements

Section 3.1.2.2 Requirement #	**Requirement Description**	**Additional Information**
1	To achieve the level of network hardening required by public safety, and to meet the availability requirements given in Section 3.4, the radio network shall use minimum best server design to identify sites that require additional hardening.	This will determine which sites will require what level of hardening per the guidance given in this Section.
2	OAM&P Robustness: There shall be no impact on established service from the non-service-affecting management commands and queries. All potentially service-affecting OAM&P activities shall require command confirmation to minimize accidental service outage	
3	Redundant/spare core equipment shall be warehoused in physically separate buildings away from hazard zones.	
4	Physical diversity shall be used for core communications and power.	
5	Buildings housing Infrastructure equipment, including at cell locations, shall meet or exceed local building codes and safety including but not limited to seismic safety standards.	

6	Cell sites shall have: Emergency backup power, site environmental, and transmission alarm and monitoring functions to ensure basic site status visibility during emergency or extra-ordinary events and incidents where cell site impairment is due to loss of power or telco backhaul circuit failure.	
7	All cell sites shall have: Quick connect-disconnect equipment and methods to replace batteries, generator, or fuel storage elements	
8	All cell sites shall have: A planned, functioning, survivable re-fueling plan with an annual review and drill exercises program	DBL and PSBL should integrate with state/local disaster recovery plans.
9	All cell sites shall have: A planned, functioning, survivable emergency generator deployment and management methodology with an annual review and drill exercise programs	

3.1.3 Recovery and Restoration

Section 3.1.3 Requirement #	Requirement Description	Additional Information
1	DBL shall address and correct any service affecting outage (any instance where 50% or more of the network capacity is affected at the sector level, 25% at points higher in the architecture) within two (2) hours, four (4) hours for any service affecting outage, and shall address any minor alarms within eight (8) hours; Rural areas shall be extended to 8 hours	
2	D-block Licensee will need to make available deployable solution for disaster recovery for use by public safety	
3	DBL must provide on-site customer support in the event of an emergency within two hours of notification.	

3.2 Reliability

Section 3.2 Requirement #	Requirement Description	Additional Information
1	The network operator must ensure data/call processing functionality is restored within a predetermined and guaranteed time period following an outage (scheduled or unscheduled) as negotiated between the PSBL and DBL.	This will generally translate into either or both capacity loss and service degradation. Reliability objectives may be drawn from "Reliability and Quality Measurements for Telecommunications Systems (RQMS-Wireless), GR -1929 from Telecordia.
3	Network operations center owned or contracted for by the network operator should operate 24x7x365 and be required to have a subset of TL9000 certification to ensure quality system management.	TL-9000 certification requirements include those of ISO-9000 plus 90 additional requirements, and have been widely developed and accepted by the communications industry, including multiple carriers and equipment suppliers.
4	The PSBL requires the network operator ensure call processing Network Element availability through engineering methodologies promoting fault tolerance and high availability, as applicable to network routing nodes, transport interconnects and application service nodes.	
5	The network should offer the capability to do basic self-recovery to expedite service restoration and/or return to redundant operation.	
6	The system shall not experience a functional or equipment failure within the agreed to and specified availability limits of the network operating environment that includes factors such climate, operational vibration, earthquake, EMI/ESD, and supplied power.	

3.3 Redundancy

The system should provide redundancy for all the critical components including but not limited to:

- Backhaul
- IP Core
- Battery backup
- Power supply units
- Base station components

Section 3.3 Requirement #	Requirement Description	Additional Information
1	In conjunction with requirement 3.1.2.1 the network design will use minimum best server design to provide overlapping site coverage as possible. This will help ensure some form of redundant coverage in case of catastrophic site failure	
2	The PSBL requires the network operator ensure call processing network element availability through engineering methodologies promoting fault tolerance and high availability, as applicable to network routing nodes, transport interconnects and application service nodes.	The system of Network Elements should offer the capability to do basic self-recovery to expedite service restoration and/or return to redundant operation. The network operator must ensure call processing functionality is restored within a predetermined and guaranteed time period following an outage (scheduled or unscheduled) where feasible to do so.
3	Where redundancy is implemented the system should automatically detect and activate components to provide service upon failures of primary network components.	

3.4 Availability

The following are provided as guidance in meeting the availability requirements that follow:

- Power backup using battery backup and/or power generators
- Redundant backhaul circuits from the RAN to the Core
- High wind loading for the cell towers
- Either highly reliable (99.999%) individual network elements or operating them in a fail-over redundant manner
- Ensuring adequate supply and easy access to spares to reduce Mean Time To Repair
- Redundant NOC with separate geographical operational locations. The backup NOC will have the ability to take over full operations during a failure or physical loss of a primary operational

NOC. Each NOC will also have redundant backbone connections to both the primary and backup NOC locations.

Section 3.4 Requirement #	Requirement Description	Additional Information
1	The network availability should be calculated as follows: $$Availability_{Net} = \frac{\sum_{i=1}^{N} Availability_i}{N * 525{,}960 - \sum_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{Planned\ Outage_i}}$$	
2	*Availability$_i$* is the availability of each service affecting network component in minutes broken down to the lowest level of service affecting component in a defined area in minutes or fractions thereof.	
3	*Planned Outage$_i$* is the total amount of minutes that each component was intentionally placed out of service for scheduled maintenance.	
4	*N* is the total number of service affecting network components, including both the RAN and accessibility to the core in that same defined area where an outage has occurred.	Excluded from the calculation are: end user devices, external networks & gateways, and the RF link - Coverage availability defined as 95%.
5	Availability of the system shall grow incrementally based on the following: Year 1 – 99.9% Year 4 – 99.95% Year 7 – 99.99% Year 10 – 99.995%	This includes disasters, but also doesn't penalize when disaster recovery methods such as emergency deployable systems are successful.

3.5 Interfaces and Interoperability

Section 3.5 Requirement #	Requirement Description	Additional Information
1	The network will support an interface to Project 25 Inter RF Subsystem Interface (ISSI) Voice Service and Supplementary Services.	
2	The network will support an interface to Project 25 Console Subsystem Interface (CSSI) Voice Service and Supplementary Services.	
3	The network will support an interface to the Public Switched Telephone Network.	

4	The network will support an interface to Integrated Services Digital Network (ISDN) Primary Rate Signaling.	
5	The network will support an interface to cellular voice networks.	Including but not limited to 3GPP and 3GPP2 networks
6	The network will support an interface to IP Multimedia Subsystem (IMS) compliant signaling.	
7	The network will support an interface to PTT signaling (whether DTMF, PoC, and/or OMA-PoC)	
8	The network will support an interface to the NIST/OLES VoIP implementation profiles.	
9	The network will support an interface to the Next Generation 9-1-1 network.	Functionality shall include: - Access to external gateways that allow the Next Generation 9-1-1 network to access and be accessed by other Emergency Responder Entities and networks in a secure fault tolerant manner. - Support multiple multi-media types as may be utilized in the Next Generation 9-1-1 network such as voice, text, pictures, video, etc. - Support secure isolation of Next Generation 9-1-1 traffic from other PSBL priority users and commercial traffic.
10	The network should support an interface to a non-terrestrial or satellite based broadband network.	
11	Network interoperability shall be done via a single national IP based radio air interface standard	With the ability to migrate to new technologies.
12	The network shall support an interface to the Internet.	
13	The network should support connections between the nationwide broadband network, local area broadband systems and local, state or regional voice and data systems	
14	The network shall be interoperable with federal systems and networks to allow connection to authorized federal databases.	

4 Application/Service Requirements

4.1 General Application/Service Requirements

This section is a catch all for requirements that are relevant to the applications/services public safety expects in the 700MHz band, but that don't easily fit in one of the other sections.

Section 4.1 Requirement #	Requirement Description	Additional Information
1	The Public Safety Broadband Licensee shall not be responsible for deploying applications and services that are national in nature, such as cellular or push-to-talk voice. Rather, the D-block licensee shall be responsible for deploying those applications/services that are national in nature.	Those applications/services that will be deployed by the DBL are designated in Section 4.2.
2	Applications and services can be deployed on the network without air-interface specific development.	i.e. an application/service can be written independently of the RAN, and still have the ability to be assigned to a QoS class of service and have priority associated with the application flow.
3	Applications/services to be deployed on the network shall require compliance with a test plan.	The test plan will be developed between a state/local agency and the PSBL for locally deployed applications/services, or a plan developed between the PSBL and the DBL for nationally deployed applications/services.

4.2 Application/Service Schedule

This section contains a table that lists the applications/services for public safety, their Quality of Service class as defined in Section 4.3, the schedule that the application/service will be deployed, and whether or not the DBL will be responsible for deploying the application/service nationally. This section does not define specific operational/user interface requirements of these application/service classes. Also, a brief description of each application/service follows this table.

Section 4.2 Requirement #	Application/Service	Quality of Service Class[1]	Year 1	Year 4	Year 7	Year 10	National
1	File transfer	5	X	X	X	X	
2	E-Mail	6	X	X	X	X	
3	Web browsing	6	X	X	X	X	
4	Cellular voice	0,2	X	X	X	X	Yes
5	Push to talk voice[2]	1,2	X	X	X	X	Yes
6	Indoor video	4		X	X	X	
7	Outdoor video	4	X	X	X	X	
8	Location Services	3	X	X	X	X	Yes
9	Database transactions, e.g. RMS	5	X	X	X	X	
10	Messaging	3	X	X	X	X	Yes
11	Operations data	6	X	X	X	X	
12	Dispatch data	5	X	X	X	X	
13	Generic traffic	6	X	X	X	X	
14	Telemetry[3]	3,5	X	X	X	X	
15	VPN traffic	3	X	X	X	X	

[1] This column maps directly to the classes of service defined in Section 4.3

[2] Typically commercial grade push-to-talk, not intended as a replacement for land mobile radio.

[3] QoS Class 3 for real-time sensors such as biometric data, QoS Class 5 for non real-time sensors.

Application/Service	Description	Data Rate[4]
File transfer	i.e. to download such items as high-resolution images, etc.	Greater than 256kb/s
Email		Less than 16kb/s
Web browsing		Greater than 32kb/s
Cellular voice	Analogous to today's cellular system capability.	4-25 kb/s
Push to talk voice	Analogous to commercial offerings, but coupled with group call capability.	4-25 kb/s
Indoor video	Indoor video is video that is transmitted from inside a building, whether it is surveillance or tactical video.	20-384 kb/s[5]
Outdoor video	Outdoor video is video that is transmitted from the street, whether it is surveillance or tactical video.	32-384 kb/s[4]
Location services	This includes location services for personnel as well as vehicles and other objects that public safety tracks.	Less than 16kb/s
Database transactions	This includes both remote databases (data that is not under the agency's direct control), as well as databases that are local.	Less than 32kb/s
Messaging	Instant messaging and SMS type services.	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.	Less than 32kb/s
Dispatch data	This area primarily covers data as it relates to computer aided dispatching.	Less than 64kb/s

[4] These figures are per application flow.

[5] It has been noted that in order to meet public safety video quality needs, the data rate will likely need to exceed 64kbps.

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.	Less than 32kb/s
Virtual Private Networking		Less than 64kb/s

Table 1 Application/Service Definition and Data Rates

4.3 Quality of Service Classes

This section defines the classes of service that public safety requires in order that their quality of service expectations are met. It is understood that given a particular radio access network technology, and per the configuration of the core, these QoS classes might need to be mapped into what the RAN and core can accommodate.

Section 4.3 Requirement #	Requirement Description	Additional Information
1	The network will support a QoS class of service for: Real-time, jitter sensitive, high interaction (cellular voice, push to talk voice, etc.).	QoS Class of Service 0
2	The network will support a QoS class of service for: Real-time, jitter sensitive, interactive (cellular voice, push to talk voice, etc.).	QoS Class of Service 1
3	The network will support a QoS class of service for: Transaction data, highly interactive (Signaling)	QoS Class of Service 2
4	The network will support a QoS class of service for: Transaction data, interactive	QoS Class of Service 3
5	The network will support a QoS class of service for: Low loss, real-time (video)	QoS Class of Service 4

6	The network will support a QoS class of service for: Low loss only (short transactions, bulk data)	QoS Class of Service 5
7	The network will support a QoS class of service for: Traditional applications of default IP networks	QoS Class of Service 6

4.4 Network Performance Values for Quality of Service Classes

This section sets the performance values for the classes of service as defined in Section 4.3. This is not an exhaustive set of parameters and values, as each application/service will require separate treatment with respect to data rates and other application specific metrics.

Network performance parameter	**Nature of network performance objective**	**QoS Classes of Service**[6]						
		Class 0	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 5**	**Class 6**
Transfer Delay	Upper bound on the mean transfer delay (edge to edge)[7]	150ms	400 ms	150ms	400 ms	400ms – 2s	1 s	U[8]
Delay Variation	Upper bound on the $1 – 10^{-3}$ quantile of transfer delay minus the minimum transfer delay	50 ms	50 ms	U	U	2 s	U	U
Loss Rate	Upper bound on the packet loss probability	Section 4.5	Section 4.5	U	U	Section 4.5	U	U

4.5 Application/Service Quality of Service Parameters and Values

The two applications/services that require a more in depth understanding regarding their quality of service requirements are audio and video. As testing has proven, the quality of service parameters for audio and video are codec dependent. Therefore, until codecs are selected for audio and video applications, the general network performance parameters and values shall be used.

[6] These figures are derived from ITU-T Y.1541.

[7] Edge to edge internal to the 700MHz network.

[8] U means unspecified or unbounded.

5 Security Requirements

The 700MHz public safety network will be used for a wide variety of applications by various agencies. In some cases, the network will be used to replace or augment existing technologies. In those situations, it is reasonable to assume that the users would expect the same security features as existing systems. In other cases, the network will be used in novel ways which may dictate differing security policies. In order to be of use to the broadest possible set of state/local agencies, the network must support a flexible security architecture. Each agency must be permitted to implement its own security policy within certain constraints, and, in some cases, multiple policies for different uses may be required by a single agency.

The hybrid nature of the network makes security particularly important since both public safety and the general public will be using devices with access to the network. For example, public safety agencies require the capability to encrypt sensitive communications and to control who has access to this information.

While there will be additional requirements, such as end-to-end encryption for particular applications, that will be met by the individual agencies or by the PSBL, the following requirements are to be met by the DBL except where otherwise designated.

5.1 Network Security

5.1.1 Access Controls

The network shall implement controls to ensure that network access is limited to authorized users and devices.

5.1.1.1 Device Authentication

Section 5.1.1.1 Requirement #	Requirement Description	Additional Information
1	The network shall require each device that attempts to connect to the network to prove its identity prior to granting access to network resources. Each device will be assigned a unique identifier, and the authentication method must provide strong assurance (e.g. by public key cryptography) of the device's identity in a manner that requires no user interaction.	

2	To protect against both malicious devices and malicious network stations, the authentication must be mutual, with the device proving its identity to the network and the network proving its identity to the device.	

5.1.1.2 Option to Authenticate User

Section 5.1.1.2 Requirement #	Requirement Description	Additional Information
1	Each state/local agency shall be granted the option to require user authentication in addition to device authentication for devices assigned to that agency. When user authentication has been selected as an agency requirement, the network shall require each device to prove its user's identity prior to granting access to network resources other than the user authentication service.	Public safety agencies expect the ability to enforce user authentication for certain types of devices (e.g. laptops and PDAs), but user authentication is impractical for other types of devices (e.g. unattended sensors or simple handheld devices that lack authentication input). User credentials may be provided to the device by various means such as a PIN or password entry interface, a hardware token (e.g. SIM), or by a biometric scanner according to the agency's requirements. This could include single sign-on granted by a device based on prior user authentication (e.g. Windows login).
2	For agencies requiring user authentication, the network must facilitate sequential authentication of multiple users from a single device.	Concurrent authentication of multiple users from a single device is not required.
3	The PSBL shall provide a password authentication service. The DBL shall provide a mechanism to authenticate users against the PSBL password authentication service. State/local agencies may choose to subscribe to this service or to implement their own network-based authentication service (e.g. to implement token or biometric systems or to provide single sign-on using existing passwords).	This interface will be provided by the PSBL.
4	For agencies that use the network's password authentication service, the agency shall be granted via administrative	

	interface (e.g. Web based) the ability to add, remove, and manage user accounts that are permitted to access the network.	
5	The PSBL shall publish and enforce a password management policy that may include requirements for password length, complexity, reuse, etc.	
6	A state/local agency that chooses to use its own authentication service shall be responsible for the implementation of that service and for selection of devices that support the service. The DBL shall accommodate this capability with an interface to the agency's authentication service.	

5.1.1.3 Authorization

Section 5.1.1.3 Requirement #	Requirement Description	Additional Information
1	Access to public safety services and applications shall be provided only to those authenticated users and/or devices as specifically authorized by the state/local agency.	The DBL shall ensure authorization only for those services provided by the DBL.
2	Each agency shall be granted control over authorization by means of an administrative interface.	

5.1.1.4 Automatic Logoff

Section 5.1.1.4 Requirement #	Requirement Description	Additional Information
1	The network shall enforce a configurable time-out, imposing a maximum time that each device may be connected to the network.	The default setting should be infinite (no time-out).
2	The network shall enforce an inactivity time-out, imposing a maximum time that each device may be connected to the network without transmitting data.	The default setting should be infinite (no time-out).
3	Each state/local agency shall be granted control of the network time-out and inactivity time-out setting for devices assigned to that agency.	The setting may be a single setting affecting all of the agency's devices.

4	Each agency shall also be granted via administrative interface the means to manually and forcibly terminate access to the network for any of its assigned devices individually.	

5.1.2 Transmission Secrecy

Section 5.1.2 Requirement #	Requirement Description	Additional Information
1	The network shall provide cryptographic controls to ensure that transmissions can only be received by the intended recipient. This must include data encryption over all wireless links.	
2	The encryption of wireless links shall utilize cryptographic modules that are certified by NIST as compliant with Federal Information Processing System (FIPS) Publication 140-2 (Level 1 minimum) for "Security Requirements for Cryptographic Modules" with a minimum key length of 128 bits.	FIPS 140-3 will be required instead of 140-2 pending finalization of the standard.
3	The encryption should support both point-to-point traffic and point-to-multipoint traffic.	
4	The network shall support periodic re-keying of devices such that traffic encryption keys may be changed without re-authentication of the device and without interruption of service.	

5.1.3 Transmission Integrity

Section 5.1.3 Requirement #	Requirement Description	Additional Information
1	The network shall provide cryptographic controls to ensure that received transmissions have not been modified in transit.	
2	The network shall provide cryptographic controls to establish that data were sent by the identified parties.	This requirement applies only to identities (e.g. MAC addresses) below the IP layer.

5.1.4 Audit Controls

Section 5.1.4 Requirement #	Requirement Description	Additional Information
1	The network shall maintain a record of all device and user access attempts and all authentication and authorization transactions, including changes to authentication and authorization data stores.	
2	These records should be maintained and stored according to information assurance best practices and protected from unauthorized access.	Any detailed records of user activity (IP destination addresses, data use profiles, etc.) should likewise be protected from unauthorized access.
3	These records of user/device transactions shall be made available to the state/local agency's authorized administrator upon request.	

5.1.5 Availability

Section 5.1.5 Requirement #	Requirement Description	Additional Information
1	The DBL shall make available to local/state agencies all contingency plans relating to jamming and other denial of service attacks.	In a shared network with both commercial and public safety users, it is imperative to prevent unauthorized users from denying service to public safety, e.g. by flooding the network with registration requests or accessing high bandwidth applications they are not authorized to use. The contingency plans shall be provided upon request via the PSBL.
2	The network shall be capable of attack monitoring.	
3	The network shall be able to survive automated network vulnerability scans (e.g. by Nessus).	

5.2 Device Requirements

5.2.1 Access Controls

Devices shall provide controls to prevent use by unauthorized users and access to unauthorized networks.

5.2.1.1 Network Authentication

Section 5.2.1.1 Requirement #	Requirement Description	Additional Information
1	Devices shall conform to the network's device authentication protocol. Each device will be assigned a unique identifier, and the authentication method must provide strong assurance (e.g. by public key cryptography) of the device's identity in a manner that requires no user interaction.	
2	To protect against both malicious devices and malicious network stations, the authentication must be mutual, with the device proving its identity to the network and the network proving its identity to the device. The device must not permit connectivity to the public safety network unless the network is authenticated.	

5.2.1.2 Option to Authenticate User

Section 5.2.1.2 Requirement #	Requirement Description	Additional Information
1	Each state/local agency shall have the option to require user authentication for device access. When user authentication has been selected as an agency requirement, the device shall require each user to prove his or her identity prior to granting access to applications or network resources other than the user authentication service.	User credentials may be provided to the device by various means such as a PIN or password entry interface, a hardware token (e.g. SIM), or by a biometric scanner according to the agency's requirements.
2	Agencies may require user authentication using the PSBL's password authentication service, using a local credential store (e.g. a per-user or per-device PIN or a biometric system with local registry), or by an agency-managed network-based authentication service.	

5.2.2 Data Protection

Devices may provide controls to protect the secrecy of data stored on devices (e.g. in the case of device loss or theft).

5.2.2.1 Secure Erasure

Section 5.2.2.1 Requirement #	Requirement Description	Additional Information
1	Devices may support a means of erasing (via best practice multiple pass overwriting of data storage media) all data stored on the device.	
2	A remote erasure service may be available whereby a state/local agency can select a device that is connected to the network and force it to erase all data stored on the device, including network access credentials.	

5.2.2.2 Option to Encrypt Stored Data

Section 5.2.2.2 Requirement #	Requirement Description	Additional Information
1	Devices may support a means of encrypting data stored on the device. Any encrypted data shall be impossible to decrypt without user authentication.	
2	The encryption shall utilize cryptographic modules that are compliant with Federal Information Processing System (FIPS) Publication 140-2 (Level 1 minimum) for "Security Requirements for Cryptographic Modules" with a minimum key length of 128 bits.	FIPS 140-3 will be required instead of 140-2 pending finalization of the standard.

5.3 Administrative Requirements

5.3.1 Security Management

Section 5.3.1 Requirement #	Requirement Description	Additional Information
1	In order to ensure network security, the DBL shall follow ISO 17799 standard practices for security management.	Administrative, technical, and physical security controls shall be selected based on analysis of risks to the security of the public safety network and to data held for or about state/local agencies.

5.3.2 Designation of Agency Authority

Section 5.3.2 Requirement #	Requirement Description	Additional Information
1	Each state/local agency shall designate one or more individuals with authority to exercise the agency options described in these security requirements.	
2	The DBL shall maintain contact information for all such individuals and must require authentication of an individual's identity before allowing changes to those options.	

5.3.3 Oversight

Section 5.3.3 Requirement #	Requirement Description	Additional Information
1	While the DBL shall have ultimate responsibility for the security of the network, the Public Safety Broadband Licensee shall be granted the ability to audit the DBL's security management and operations on behalf of state/local agencies.	
2	The findings of any such audit shall be made available to all state/local agencies.	The findings shall be provided upon request via the PSBL.
3	The DBL's security policy shall be made available to all state/local agencies.	The policy shall be provided upon request via the PSBL.

5.3.4 Incident Management

Section 5.3.4 Requirement #	Requirement Description	Additional Information
1	A procedure for managing security breaches or other incidents that may impact the security of the network or state/local agencies shall be developed and documented by the DBL.	
2	In addition to tracking each incident and mitigating harmful effects to a reasonable extent, the incident response procedure must include timely reporting of each incident to the affected agencies.	

5.3.5 Privacy

Section 5.3.5 Requirement #	Requirement Description	Additional Information
1	All applicable Federal, State and Local laws shall be adhered to in securing the privacy of individuals' information throughout the information's lifetime.	
2	Any personal data, including information about employees, members of the public, organizations and business partners, collected and maintained by the DBL will only be used for the stated purpose for which it was gathered and may not be shared, except where required by the applicable laws, unless the individual's permission is acquired.	

6 Device Requirements

6.1 *General Requirements*

Section 6.1 Requirement #	Requirement Description	Additional Information
1	The PSBL seeks from the DBL devices that are readily available on the commercial markets today.	The expectation of public safety is that the DBL will leverage its collective buying power on behalf of the public safety community in purchasing user devices.

6.1.1 Software

6.1.1.1 Operating Systems

Section 6.1.1.1 Requirement #	Requirement Description	Additional Information
1	For personal computing platforms, at least one device per device class in Section 6.2 will support the three largest operating systems (by market share of the government/industrial users). Families of operating systems (e.g., Windows 2000, Windows XP and Windows Vista) shall be considered a single operating system in regards to this requirement.	There is no requirement that a single device must support all three operating systems. This requirement can be accomplished using multiple devices of a single device class.
2	For personal computing platforms, the devices will support any operating system with 10 percent or more market share.	The same qualifiers of #1 above apply.
3	For personal computing platforms, the legacy version of that operating system will be supported for a period of three years after the release of the new operating system (e.g., Windows XP must be supported for at least three years from the date of Vista availability).	
4	For personal computing platforms, new operating systems must be supported within six months of the launch of that operating system.	

5	For personal digital assistants (PDA), the devices will support the three largest operating systems (by market share of government/industrial users). Families of operating systems (e.g., Windows Mobile 5.0 and Windows Mobile 6.0) shall be considered a single operating system in regards to this requirement.	There is no requirement that a single device must support all three operating systems. This requirement can be accomplished using multiple devices of a single device class.
6	For PDA's, the devices will support any operating system with 10 percent or more market share.	The qualifiers of #5 above will also apply here.
7	For PDA's, the legacy version of that operating system will be supported for a period of two years after the release of the new operating system.	
8	For PDA's, new operating systems must be supported within 6 months of the launch of that operating system.	
9	For PDA's, the operating system will be bundled with the device.	

6.1.1.2 Access Security

Section 6.1.1.2 Requirement #	Requirement Description	Additional Information
1	At least one handheld phone and PDA option shall be capable of password and/or biometric access to the device.	
2	At least one handheld phone and PDA shall provide some limited function even if disabled (e.g., 911 calls, emergency button, and emergency messaging) to be further defined at a later time.	This capability is required in the event that another first responder needs emergency access to a public safety user's device.

6.1.2 Special Interface Options

Section 6.1.2 Requirement #	Requirement Description	Additional Information
1	The following special interfaces are required for at least one device in the phone and PDA device classes. • There must be a button that can be used as an emergency button and is fully available to the PSBL for third party application development, and • The device must have an available button for push-to-talk that is fully available for third party applications.	

6.1.2.1 Other

Section 6.1.2.1 Requirement #	Requirement Description	Additional Information
1	Public safety must be able to implement and utilize any application on a device with appropriate testing based on a process as determined by the PSBL.	
2	Public safety must be able allowed to access and utilize any capability of the device without any restrictions.	

6.1.3 Rugged

Section 6.1.3 Requirement #	Requirement Description	Additional Information
1	Any device specified in this section as “rugged” must meet MIL-810F specifications for dust, salt, rain, immersion, vibration/drop, and shock resistance	

6.1.4 Geo-location

Section 6.1.4 Requirement #	Requirement Description	Additional Information
1	A subset of the public safety devices described herein must include a GPS receiver with assisted capabilities from the 700 MHz broadband network itself.	

6.1.5 Power

See “Device Types” section for specifics.

6.1.5.1 Chargers

The following specifications apply to handheld portable devices that are battery powered.

Section 6.1.5.1 Requirement #	Requirement Description	Additional Information
1	Battery Chargers for all portable devices shall have the following features: Drop in charger, Capable of charging standard batteries to full capacity within 90 minutes, Auto-shut-off feature that stops charging the battery when it has reached full charge, Available with an integrated capacity testing-feature	
2	Battery Chargers powered from 120 VAC 60 Hz shall be available in single and multi-unit chargers	
3	Single unit vehicular chargers powered from 12 VDC shall be available.	
4	Single chargers should be available via USB host connectivity. Charging in this instance does not have to meet the time requirement in #1 above.	

6.1.5.2 Battery Life

Section 6.1.5.2 Requirement #	Requirement Description	Additional Information
1	Battery operation time for handheld devices shall be no less than 8 hours at 5% Transmit, 5% Receive, and 90% Standby (for push to talk mode) and 120 minutes talk time (cell phone mode). Extended battery life should be available for extended shifts.	Standby is defined as a device that is immediately available for transmit and receive, but is not actively transmitting or receiving.

6.1.6 RF

6.1.6.1 Sensitivity

Section 6.1.6.1 Requirement #	Requirement Description	Additional Information
1	For each class of device, all devices must meet the sensitivity specifications for the device used to approve and test for coverage and capacity verification.	See Device types for more information.

6.1.6.2 Output Power

Section 6.1.6.2 Requirement #	Requirement Description	Additional Information
1	For each class of device, all devices must meet the output specifications for the device used to approve and test for coverage and capacity verification.	

6.1.6.3 Interference

Section 6.1.6.3 Requirement #	Requirement Description	Additional Information
1	Network devices used in recommended configurations should not harmfully interfere with radios in the adjacent narrowband 700MHz channels – either a portable worn by the same user, or vehicle radio used in the same vehicle.	

6.1.7 Other

Section 6.1.7 Requirement #	Requirement Description	Additional Information
1	The network shall provide sufficient backwards compatibility such that in no case the device would require replacement within 3 years of the sale of that device.	

6.2 Device Types

Section 6.2 Requirement #	Requirement Description	Additional Information
1	D-block licensee shall provide at least one, but preferably two types of each of the following devices.	

2	Unless otherwise noted, the device shall be a Class 3 device as specified in Section 7.1.2.	

6.2.1 Field Replaceable Modem Cards

This section deals with subscriber device requirements for field replaceable modem cards

6.2.1.1 PCMCIA

Section 6.2.1.1 Requirement #	Requirement Description	Additional Information
1	DBL must supply a PCMCIA version device for a period of three years beyond their last availability in new ruggedized notebook computers (of the top three ruggedized computer vendors).	The PCMCIA form factor and standard is being superseded by the ExpressCard format (see below). This requirement seeks to ensure that public safety does not get stranded with expensive computing platforms.

6.2.1.2 PC ExpressCard

Section 6.2.1.2 Requirement #	Requirement Description	Additional Information
1	DBL must provide both 34mm and 54mm wide PC ExpressCard versions.	

6.2.1.3 USB Modem

Section 6.2.1.3 Requirement #	Requirement Description	Additional Information
1	DBL must provide a modem with a USB interface.	

6.2.2 Embedded Devices

Section 6.2.2 Requirement #	Requirement Description	Additional Information
1	D-block must make available to computer manufacturers embedded modem solutions that can be factory installed in rugged and non-rugged computers.	
2	The solution must be available on no less than three notebook computer vendors and three ruggedized notebook computer vendors.	There is no requirement that these devices are interchangeable between vendors, and the form factor is not standardized.

6.2.3 AVL Modem

Section 6.2.3 Requirement #	Requirement Description	Additional Information
1	All devices in this class must provide GPS capabilities that are available to both the device and the network	The AVL Modem is a device envisioned to provide connectivity to an on-board computer and to autonomously send geo-location information to a third party software application to track the unit.
2	This unit must support the major geo-location protocols.	
3	The unit must offer mounting brackets for forward compartment or trunk mounting capabilities, for 12VDC negative-ground vehicle systems.	
4	The unit should allow for local on/off control via physical switch or software command from the vehicle end-user device.	
5	The unit should offer Ethernet and USB connectivity.	
6	The unit must be rugged as defined above.	

6.2.4 High Power Modem

Section 6.2.4 Requirement #	Requirement Description	Additional Information
1	At least one high power modem shall be made available to public safety. This device will be a Class 1 device as defined in Section 7.1.2.	
2	The modem shall meet the requirements outlined above in the “AVL Modem” section, and shall also have higher power capability.	
3	The high power modem should meet rugged specs outlined above and offer mounting brackets for forward compartment or trunk mounting capabilities, for 12VDC negative-ground vehicle systems.	
4	The high power modem should allow for local on/off control via physical switch or software command from the vehicle end-user device.	

5	The high powered modem must include an integrated GPS receiver with the same capabilities as the AVL modem above as an option.	

6.2.5 Personal Digital Assistant (PDA)

Section 6.2.5 Requirement #	Requirement Description	Additional Information
1	DBL shall provide a personal digital assistant device that has the prevailing capabilities of the current personal digital assistants of the time (e.g., camera, phone, PIM, email, web browser, messaging capabilities).	
2	At least two form factors will be provided: one will include the QWERTY keypad on the same plane as the screen, the other will allow for a slide out keyboard.	
3	Compliant PDAs should be available from at least two vendors.	

6.2.6 Rugged PDA

Section 6.2.6 Requirement #	Requirement Description	Additional Information
1	DBL shall provide at least one rugged PDA that meets both the PDA and rugged requirements above.	

6.2.7 Cell Phone

Section 6.2.7 Requirement #	Requirement Description	Additional Information
1	DBL shall provide cell phone form factors with the same capabilities and form as is provided in the commercial marketplace and with the same features available in a cell phone.	It is understood that a cell phone does not include a QWERTY keypad as does a PDA, but otherwise, it can support other capabilities as is consistent with the prevailing phone capabilities in the commercial marketplace.

6.2.8 Rugged Cell Phone

Section 6.2.8 Requirement #	Requirement Description	Additional Information
1	DBL shall provide at least one rugged cell phone that meets both the Cell Phone and rugged requirements above.	

6.2.9 Other Devices

The BBWG anticipates that the PSBL will fully develop market specific public safety devices directly with the vendor community. This section will be the future home for the requirements of those future devices.

Section 6.2.9 Requirement #	Requirement Description	Additional Information
1	Other devices/device types that are not represented above also need to be supported. However, these requirements do not apply to those devices and DBL must fully specify all necessary standards for PBSL to bring other devices on the network.	

6.3 Satellite Devices

At least one user device will need to offer dual mode operation between the 700 MHz broadband network and satellite provider service. The satellite service provider shall provide coverage in the USA – including Hawaii and Alaska.

Section 6.3 Requirement #	Requirement Description	Additional Information
1	The satellite capable device must have integrated broadband 700 MHz and satellite capabilities.	Other 700MHz devices providing satellite access via a short range connection to a portable satellite companion device should be considered.
2	The device must allow for automatic connection to satellite services upon loss of service at 700 MHz. Expectations for transition from broadband to satellite are TBD.	Automatic switch to satellite operation upon loss of service is fine, but seamless in-call transition is not recommended: real time synchronous traffic switching between satellite and terrestrial networks adds cost/complexity/risk which runs counter to the goal of maintaining a high availability capability in disaster scenarios.

3	Device capabilities must include (but are not limited to) voice, GPS, email, and web browsing over both 700 MHz and satellite data connections	All services are available over satellite connection but for reasons of spectral efficiency and link margin, packet switched data/video services is preferred to be provided via sub-notebook size directional antenna companion device or steerable antenna mobile terminal. Handheld and PDA devices limited to voice/GPS/PTT/messaging in satellite mode.
4	The device must meet the Personal Digital Assistant requirements specified in 6.2.5 above.	Basic satellite voice/GPS/PTT/low rate messaging via PDA form factor device. Broadband packet switched data with QoS via note-book size directional antenna companion device or steerable antenna mobile terminal.
5	The device must meet above rugged requirements defined in Section 6.1.3	
6	The device must allow for a standard interface for a satellite modem card to allow the PSBL flexibility to later choose a satellite service provider. However, the DBL, must provide devices that have integrated modems upon selection of a service provider. The PSBL must also have flexibility to later change service providers, and therefore, standard modem cards.	

7 Network Requirements

Section 7 Requirement #	Requirement Description	Additional Information
1	The Network shall provide seamless coverage (via handoff/handover mechanisms) and continuous connectivity within the 95th percentile coverage area at stationary and vehicular speeds up to 120 miles per hour.	
2	The Network configuration shall be documented by the Network operator and used as a basis for compliance verification to the PSBL requirements.	
3	The PSBL shall be notified in advance of any service affecting network changes. The advance notification time period will be negotiated between the DBL and PSBL.	
4	The Network Operator shall establish a joint program to identify Public Safety user requirements affecting the network technology roadmap and support the respective standards development organizations (SDO) process to make the requirements part of subsequent technology releases.	

7.1 Radio Network Behavior

Section 7.1 Requirement #	Requirement Description	Additional Information
1	By year 4, the network shall support a one way radio access network latency of less than 50 milliseconds. This shall be determined to be measured from mobile device to mobile device/fixed server or device or network to network.	

2	Dense Urban: Population Density +15000 people per square mile Classified as a business district including: • skyscrapers • high rise apartments • buildings of +20 stories • narrow streets	Shall use the following morphology classes to determine the classification of a county, township or parish and it will be based on the most current U.S. Census Bureau data. Problems defining such areas due to issues such as day time population versus night time and other unique situations shall be handled on a case by case basis between the PSBL and DBL.
3	Urban: Population density equal to or greater than 5000 and less than or equal to 14999 people per square mile Classified as an office/residential district including • hotels • hospitals • buildings of 4 to 19 stories • medium to narrow streets	Shall use the following morphology classes to determine the classification of a county, township or parish and it will be based on the most current U.S. Census Bureau data. Problems defining such areas due to issues such as day time population versus night time and other unique situations shall be handled on a case by case basis between the PSBL and DBL.
4	Suburban: Population density equal to or greater than 200 people per square mile and less than or equal to 4999 people per square mile. Classified as a small business/residential district including: • buildings of 1 to 3 stories • medium width streets	Shall use the following morphology classes to determine the classification of a county, township or parish and it will be based on the most current U.S. Census Bureau data. Problems defining such areas due to issues such as day time population versus night time and other unique situations shall be handled on a case by case basis between the PSBL and DBL.

5	Rural: Population density equal to or greater than 5 people per square mile and less than or equal to 199 people per square mile. Classified as a sparsely populated residential area including: • large open spaces • isolated highways • 1 to 2 story houses • Barns	Shall use the following morphology classes to determine the classification of a county, township or parish and it will be based on the most current U.S. Census Bureau data. Problems defining such areas due to issues such as day time population versus night time and other unique situations shall be handled on a case by case basis between the PSBL and DBL.
6	Highway Population density less than or equal to 4 people per square mile. Classified as stretches of interstate highway and/or US highways, principally within rural, extremely under-populated areas.	Shall use the following morphology classes to determine the classification of a county, township or parish and it will be based on the most current U.S. Census Bureau data. Problems defining such areas due to issues such as day time population versus night time and other unique situations shall be handled on a case by case basis between the PSBL and DBL.

7.1.1 Operational Frequency Range

See FCC 2nd R&O information.

7.1.2 Minimum RF Requirements

Section 7.1.2 Requirement #	Requirement Description	Additional Information
1	A single common air interface (CAI) will be utilized for the nationwide 700 MHz broadband network. This CAI will allow migration to future technology upgrades as determined by the PSBL and DBL.	
2	The network shall operate in a licensed frequency band through a combination of the D block and PSBL Broadband block. • Base station transmit frequency = 758 – 768 MHz • Base station receive frequency = 788 – 798 MHz	

3	The base station power spectral density shall not exceed 1 kW (60 dBm) ERP in any 1 MHz segment for urban and suburban areas	
4	The base station power spectral density shall not exceed 2 kW(63 dBm) ERP in any 1 MHz segment for rural areas	
5	The peak-to-average ratio shall be limited to 13 dB based on average base station transmit power	
6	RAN shall utilize maximum frequency reuse efficiency. E.g. N=1	
7	Mobile/portable station nominal transmit power shall be 0.25W ERP (24 dBm) and shall not exceed 3 W ERP (34.8 dBm) in rural areas.	Suggest Mobile Power Classes: Class 1 = 3W ERP (34.8dBm) Class 2 = 1.2W ERP (30.8 dBm) Class 3 = 0.25W ERP (24 dBm) Network design should be based on use of 0.25W (24 dBm) devices

7.1.2.1 RF Interference Requirements

Section 7.1.2.1 Requirement #	Requirement Description	Additional Information
1	The 700 MHz Nationwide Public safety Broadband Network must be designed to avoid interference to the public safety 700 MHz Narrowband spectrum blocks at 769-775 MHz and 799-805 MHz.	The network operator shall use best care practices to mitigate inter-modulation, receiver de-sense or other "near-far" issues. This may include but not be limited to coordinating site locations or broadband signal levels at ground level in close proximity to base stations.
2	The DBL and PSBL shall create a process to expeditiously resolve interference issues that are identified.	The NSA will specify provisions defining responsibility to resolve interference, should it occur, and the level of protection to be provided
3	The out-of-band emission (OOBE) within the 700MHz public safety narrowband band (769 – 775 MHz and 799 – 805 MHz) should be attenuated to at least 76 + 10log P into a 6.25 kHz bandwidth.	

7.1.3 Coverage

Section 7.1.3 Requirement #	Requirement Description	Additional Information
1	D Block licensee to provide signal coverage and offer service to: Year % Population Coverage 2010 15% 2011 35% 2012 55% **2013 75%** 2014 85% 2015 90% **2016 95%** 2017 96% 2018 97% **2019 99.3%** Communities in excess of 3,000 are part of the build out as are all major US highways and interstates.	Based on the most current U.S. Census Bureau data.
2	Corridors are defined as Interstate Highways and US Highways. Coverage threshold minimums for these corridors should extend beyond the physical corridor.	Actual coverage area will be determined on a case by case basis between the network operator and PSBL.
3	The network shall be designed to meet or exceed the population coverage milestones stipulated by the FCC for the PSBL.	
4	Geographic coverage shall be measured by the network operator each calendar year using capture and data analysis and reporting methods agreed to by the PSBL.	A annual joint review of the coverage data shall be held between the PSBL and the network operator to determine the extent of PSBL priority user coverage, provide a method to the PSBL to provide input to the network operator for coverage enhancements and expansion, and to enable the PSBL to communicate the availability of coverage to its network priority user "customers".

5	The network operator and PSBL shall negotiate on a case by case basis for all specific, targeted, or enhanced in-door coverage. These include but are not limited to coverage for difficult areas such as tunnels and underground.	These areas shall be exempt from in-building penetration requirements.

7.2 System and User Coverage, Capacity and Data Rate

The following criteria were used to determine a normalized system model. These numbers are an average across several technologies and are not meant to specify any one radio access technology.

Pedestrian Model		BTS	2 Branch Diversity
Coverage Availability	95%	BTS Antenna Height	
Mobile Tx	24 dBm	Rural	50m
Body Loss	3 dB	Suburban	35m
UE Antenna Gain	-2 dBi	Urban	35m
Net Mobile EIRP	19 dBi	Dense Urban	25m
		BTS Antenna Gain	14 dBi
Indoor Log Normal STD	8 dB	BTS Noise Figure	5 dB
Band Width	5 MHz	Feeder Loss	3 dB
Sector Load	70%		

The network shall support the following link budget: Morphology	In-Building Penetration Margin	Coverage Availability	Net Mobile TX - EIRP	On street - Single user peak edge forward link throughput	On street - Single user peak edge reverse link throughput
Dense Urban	22 dB	95%	19 dBm	1000 kbps	256 kbps
Urban	19 dB	95%	19 dBm	1000 kbps	256 kbps
Suburban	13 dB	95%	19 dBm	512 kbps	128 kbps
Rural	6 dB	95%	19 dBm	512 kbps	128 kbps
Highway	6 dB	95%	19 dBm	128 kbps	64 kbps

On street = “in the clear”

Typical sector throughput will be approximately 5 Mbps on the downlink and 3 Mbps on the uplink. This capacity number will vary according to specific site build out, morphology and various other factors and is only meant as a system guideline for capacity.

Coverage shall be measured in the following manner: Within a defined township, parish or county

NOTE: Table above is for first two years of operation. The network will deliver incremental improvements to throughput consistent with overall CMRS (Commercial Mobile Radio Service i.e. cellular service providers) industry throughput improvements. These throughput improvements will be measured at years 4, 7, and 10."

7.3 Radio Access Network Features

Section 7.3 Requirement #	Requirement Description	Additional Information
1	The Network shall support downlink Broadcast and Multicast over multi-cell area via synchronous transmissions.	
2	The Network shall provide a group data startup time, from source node to distribution through the network of less than 2 seconds.	
3	The Network shall provide Quality of Service for Group and Broadcast traffic.	

4	The Network shall support intra-system handoffs or handover between sites and/or systems	Handoff/Handover should be seamless to the end user.
5	The RAN in general should support a high-data-rate, low-latency and packet-optimized radio-access technology.	
6	The system shall support Over the Air Programming (OTAP) for terminal configuration updates for new features and for firmware changes.	

7.4 Capacity Requirements

7.4.1 Radio Access Network Capacity

Section 7.4.1 Requirement #	Requirement Description	Additional Information
1	The system should provide the capability to set the thresholds for allowed data throughput a user/group can get.	
2	The backhaul capacity shall be designed into the network should exceed the capacity of the NodeBs/Base stations as to prevent backhaul blocking.	
3	The system shall support multiple Node B/Base station variants including but not limited to macro BTS, outdoor BTS and femtocells.	
4	The network should provide a mechanism for capping the maximum data throughput a user can get (public safety service should not be cut off – requires notification on occurrence and may affect services fees).	Rate capping control mechanisms shall be provided to the PSBL.

7.4.2 IP Core Network Capacity

Section 7.4.2 Requirement #	Requirement Description	Additional Information
1	The IP Core should provide a mechanism for alerting and reporting the maximum data usage per month per user (public safety service should not be cut off – requires notification on occurrence and may affect services fees).	

2	PSBL shall have the ability to operate and maintain a separate subscriber/user database.	
3	The IP Core Network should provide edge to edge (within the IP core) latency of less than 75 ms.	Edge to edge is defined as end-to-end round trip system latency (from the client to a server in the core and back to the client).
4	The IP Core Network should be able to utilize standard IP Network Elements (e.g. routers, switches)	

7.5 Core Network Features

Section 7.5 Requirement #	Requirement Description	Additional Information
1	The IP Core Network shall be compliant with IPv4	
2	The IP Core Network shall have the capabilities to migrate to IPv6	Migration will need to minimize cost and complexity to the end users.
3	The IP Core Network shall provide interfaces to deploy mechanisms such as but not limited to: Mobile VPN, packet compression and end-to-end secure tunneling that enhance the efficiency and security of the network.	
4	The IP core shall support NDIS - Network Driver Interface Specification	
5	The IP core network shall provide migration to a simplified user plane. This may include but is not limited to support independent scaling of control plane, user plan, IP transport and mobility management	
6	The IP core network will provide mechanisms for segmentation or redirection of traffic as needed to maintain throughput when traffic levels are high or when RAN sites are down	
7	The IP Core shall provide support for static IP addressing	

7.6 Prioritization, Quality of Service, and Pre-Emption

This section of the requirements deals specifically with prioritization of user access to the radio access network and core, quality of service requirements for user application/services, and the pre-emption of secondary users when needed by public safety.

Section 7.6 Requirement #	Requirement Description	Additional Information
1	The network shall be configured to provide the priority and Quality of Service (Section 7.5.4) management required by the requirements contained within this document in order to meet or exceed those requirements.	This requirement, and the subsequent requirements, applies to both the radio access network as well as the network core unless specified.
2	The Public Safety Broadband Licensee and network operator shall establish an appropriate service and priority framework and process that maps service and priorities to the appropriate class of service parameters that are defined in this requirements document (Section 4.4).	
3	The network operator shall identify and document the configuration parameters for the deployed broadband technology to provide the specified classes of service for the public safety services and applications.	This document shall be provided to the Public Safety Broadband Licensee.
4	The QoS metrics and priority levels must be configurable by an appropriately authorized administrator dynamically.	e.g., changing QoS metrics and prioritization at an Event/Incident scene. Profiles of users will be determined by state/local agencies in coordination with the PSBL/DBL. These user assigned profiles will be accessible by authorized, designated local administrators.

7.6.1 Priority Levels

This section provides for public safety to have priority in the RAN and core, specifies the number of levels, and speaks to state/local control over priority.

Section 7.6.1 Requirement #	Requirement Description	Additional Information
1	Priority service shall allow for different levels of service to be defined based on the given role of a user. The levels of priority will accommodate priority access to the radio access network and priority access to resources in the core network.	
2	Public safety requires 50% or a minimum of 8 access priority levels based on the number of priority levels available in the radio access network technology. These public safety priority levels are the highest levels available, over and above those levels available to commercial users.	
3	The highest priority level shall be reserved for use by public safety for emergency communications, e.g. an emergency button.	All public safety, regardless of rank or organization, shall be permitted to use this level.
4	The remaining priority levels shall be determined by state/local control.	This allows for state/local control over how an agency assigns priority to users/groups.
5	The network operator shall be able to distinguish between public safety traffic and commercial user traffic.	
6	Public safety requires priority allocation of radio access network and network core resources.	This priority allocation will leverage the same user priority levels used to access the RAN.
7	Public safety will never be blocked by commercial users in accessing the radio access network. For example, a separate public safety control channel may be needed to satisfy this requirement.	
8	The network shall provide an appropriate priority to 9-1-1 calls that may use public safety priority treatment.	

7.6.2 Logging and Records

This section provides a requirement for logging certain aspects of a public safety application/service.

Section 7.6.2 Requirement #	Requirement Description	Additional Information
1	The network shall support the ability to log the time, duration, success/failure of connection, volume of data transferred, and Quality of Service metrics of all public safety traffic.	

7.6.3 Limitation of Priority

This section provides scope limitations of priority for public safety applications/services and devices.

Section 7.6.3 Requirement #	Requirement Description	Additional Information
1	Traffic that exits the 700MHz broadband network shall not receive priority treatment.	This requirement holds unless a public safety agency or the PSBL has an agreement with another service provider to maintain priority treatment.
2	Public safety user priority is not device specific.	

7.6.4 Quality of Service

This section defines the quality of service requirements for both the radio access network as well as the network core. Additionally, it also contains requirements for application/service quality of service profiles.

Section 7.6.4 Requirement #	Requirement Description	Additional Information
1	Quality of Service shall refer to resource reservation control mechanisms. QoS mechanisms shall provide different levels of performance to a data flow in accordance with the application/service's predefined class of service.	
2	The network must support the classes of service defined in this document. Within each class of service, the network must support assignment of QoS metrics such as bandwidth, latency, jitter, and packet loss, for different classes of applications as defined in Section 4.2.	

3	The assignment of network resources must take into account both the user priority as well as the QoS requirements of the application.	Assignment of users to various priority levels and allocation of QoS metrics to different application classes will be configurable by an authorized network administrator.
4	The network shall support multiple QoS flows between a user device and network, where each flow may have a different QoS requirement and priority level.	
5	The network shall maintain a profile for each public safety user. This profile specifies the applications/services and QoS levels for those applications/services the user is authorized to for, and the priority level through which that user will communicate.	
6	The network shall allow seamless delivery of negotiated QoS during handoff.	
7	The network shall support the capability of having different QoS metrics associated with the forward and reverse airlinks.	
8	The network shall allow a user device to communicate with the network to request a reservation of the necessary resources to meet the QoS metrics associated with an application/service.	
9	If network resources are not available to meet a resource reservation request, the network shall have the ability to negotiate a mutually acceptable QoS with the user device.	The user device’s request for network resources may be limited by network operator policy and/or the user’s profile.

7.6.5 Pre-Emption

This section covers pre-emption from a general perspective.

Section 7.6.5 Requirement #	Requirement Description	Additional Information
1	In the event that the network bandwidth in the public safety portion of the network is not available or is congested due to commercial use, the network must provide a mechanism to accommodate public safety users by preempting commercial users	Note that 9-1-1 calls shell not be preempted.

8 Off Network Communications

In order to achieve the required 100% communications, several solutions may be employed:

1. Portable/fixed deployable base stations (e.g., femtocells) may be used to extend the reach of the network where coverage or capacity is limited (in coordination with the DBL and PSBL)

2. Emergency deployable systems (switching and base station functions all together in the same platform) may be used where no service exists (e.g., due to large scale outage or general lack of coverage in a rural or remote area) (from either the DBL or state/local agencies)

3. Off-network capabilities will enable subscriber devices to communicate directly with one another in the absence of infrastructure.

4. Hybrid devices (e.g. 700MHz narrowband / 700MHz broadband dual mode devices)

Specific requirements in regard to off-network communications for the DBL include:

Section 8 Requirement #	Requirement Description	Additional Information
1	The DBL will enable use of the 700 MHz public safety spectrum for off network communications. This will require various mechanisms to ensure this use does not cause harmful interference.	Other mechanisms may be used; however, public safety reserves the right for off-network activities in the 700 MHz band.
2	Direct mode subscriber devices will use up to, but not more than, 3 Watts output power.	
3	D-block licensee will support PSBL in standards bodies and with subscriber device vendor community to help achieve this requirement.	

Note: Eventually, this section will provide additional requirements that further define the need and will likely be linked to devices that are needed to satisfy off-network requirements.

Appendix A. Glossary/Acronyms[9]

Radio access network	A Radio Access Network typically consists of Node B/Base Station Transceiver, Backhaul, Base Station Antennas, and an RNC/BSC/SAE
IP Core	An IP Core typically consists of a PDSN, SGSN/GGSN, SAE, and an IMS
DBL	D Block Licensee: the entity with the highest bid in the D-Block 700 MHz auctions. Also applies, when appropriate, to the entity that successfully negotiates a Network Sharing Agreement with the Public Safety Broadband Licensee
PBSL	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.
MS	Mobile Station: any subscriber device that connects, over the air, to the 700 MHz Broadband Network in any way. This includes subscriber devices that can act autonomously, those that require manual intervention to connect, those that are handheld, those that require a host computing device, etc.
BBN	Broadband Network: the collection of devices and systems needed to deliver the required services
Local Public Safety	Any public safety entity at the county, city, state, regional, or critical infrastructure level (as determined by the PSBL).
IMS	IP Multimedia Sub-system
RNC	Radio Network Controller
SGSN	Serving GPRS Support Node
GGSN	Gateway GPRS Node
SAE	System Architecture Evolution
BSC	Base Station Controller
PDSN	Packet Data Serving Node
GPRS	General Packet Radio Service

[9] Note that none of the acronyms used in this document are intended to imply a technology choice. Rather, they are used as a method of framing the requirements using industry common terminology.

Appendix B. References

PS SoR Volume I, Version 1.2, 2006	"Public Safety Statement of Requirements for Communications and Interoperability," Volume I: Qualitative, Version 1.2, August 18, 2006
PS SoR Volume II, Version 1.0, 2006	"Public Safety Statement of Requirements for Communications and Interoperability," Volume II: Quantitative, Version 1.0, August 18, 2006
Project 34 User Needs Committee	"Project 34 User Requirements for Incident Area Networking," Version 0.3, October 31st, 2006
Project 25 User Needs Committee	"APCO Project 25 Statement of Requirements," August 4th, 2007
Project MESA	"Project MESA; Service Specification Group – Services and Applications; Statement of Requirements (SoR)," ETSI TS 170 001 V3.2.1, February 2006
Project MESA – Focus Groups	"Project MESA Functional Requirements; User Validation – Focus Group Requirements Matrix," October 21st, 2007
Office of the Chief Technology Officer of the District of Columbia	"Request for Proposal; National Capital Region Interoperability; Wireless Broadband Networks," August 7th, 2006
Counties of Suffolk and Nassau, New York	"Wireless Broadband Initiative RFP," January 17th, 2007
Department of Information Technology and Telecommunications, NYC	"Request for Proposals (RFP) Citywide Mobile Wireless Network," March 24th, 2004
National Public Safety Telecommunications Council	"NPSTC 700MHz Questionnaire Results - Final Analysis," June 12th, 2007