Public Safety

700MHz Broadband

Statement of Requirements

Version 0.6

November 8th, 2007

Table of Contents

1 Scope

The Broadband Working Group of the National Public Safety Telecommunications Council (NPSTC) has compiled the attached document to assist with the development of a nationwide interoperable broadband network for public safety agencies. This work was undertaken following the decision of the Federal Communications Commission (FCC) to establish a Public Safety Broadband Licensee (PSBL), and reflects the outcome of a first opportunity to solicit and develop public safety broadband requirements. The PSBL will be responsible for administering the 700 MHz public safety broadband segment. It will join with the D Block licensee to forge a public-private partnership to deploy and maintain the network, initially by negotiating a Network Sharing Agreement that must ultimately be approved by the FCC. The document was prepared for the many interests involved: the yet to be named PSBL, prospective D Block auction bidders, public safety agencies, equipment and infrastructure manufacturers and service providers, and the FCC. The law places ultimate responsibility with the FCC for how this spectrum is used. It is intended to communicate the network functions and characteristics the public safety community finds necessary for a network that public safety agencies will participate in and rely upon.

The effort commenced with the underlying premise that the innovation accompanying modern communications must embrace the standards associated with around the clock operations and coverage wherever a critical incident, large or small, is found. Bringing about advanced services and a nationwide interoperable network requires understanding that the citizen confronting an emergency relies on first responders and their communications capability no matter what the circumstance. Success is measured in the speed and quality of response. At stake is not only agency participation, but the public's trust in their emergency services.

The information is drawn from the experience of individuals responsible for public safety communications across varied agencies, geographies and demographics. It reflects the experience associated with single incidents to large catastrophic events. Designing, deploying and maintaining systems that continue to function throughout an emergency is the foundation of their responsibilities.

By enumerating core requirements, the Working Group's effort has been directed toward delineating what public safety has conveyed to be essential for their users. The work recognizes the reality that implementation of features, functions and performance standards will be neither immediate nor without challenge. The work recognizes the involvement of the many interests that must forge a cooperative alliance for each to succeed, such as the Network Sharing Agreement to be negotiated between the PSBL and D Block auction winner.

The Working Group sought and obtained meaningful participation from a range of public safety agencies, potential D Block auction bidders, infrastructure and equipment manufacturers and service providers, and others with experience in public safety communications. It held multiple meetings for commercial and public safety input, including a two day forum in Colorado (attendee list attached) and two days of web meetings for public safety's final review of the draft. It invited review and comment of

a draft document from over 256,000 public safety users and considered all of the over 400 comments submitted. To promote a document capable of moving a public safety broadband network used by the range of agencies closer to reality, the Working Group sought to bring clarity and comprehension to the many issues.

This document reflects a sincere commitment to make a meaningful contribution to overcoming the challenges ahead faced by the FCC, the PSBL, the D Block licensee and others in deploying and maintaining an interoperable nationwide public safety broadband network. Whether these challenges are met will in the end be judged by how expeditiously and competently assistance can be dispatched to the citizen facing an emergency, and the effective exchange of information with responding officers.

The public safety community is referenced throughout this document for the sake of brevity as "public safety." A broad view of public safety is intended wherever this reference is made. This includes all state, local, tribal, regional, and all other entities that satisfy the FCC's definition of public safety or the delegates of these entities.

1.1 Change Log

Version	Date	Changes
0.1	October 22nd, 2007	This was the first complete draft created for vetting by the NPSTC Broadband Working Group.
0.5	October 26th, 2007	This is the draft that will go out for public safety review.
0.6[1]	November 8th, 2007	This version incorporates public safety review and is the version presented to the NPSTC governing board for publication.

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

[1] Note that the Devices Section was removed from this document and will be published in a different format.

2 Operational Requirements

2.1 Support

Section 2.1 Requirement #	Requirement Description	Additional Information
1	The DBL shall provide the PSBL (or its designated entity) 24-hour, 7 days-a-week (24/7) support for fixed and user equipment. The DBL shall not be responsible for user equipment procured independently by individual agencies (with the exception of any warranties provided by DBL).	
2	The DBL must provide 24/7 operations to include field based support as necessary to maintain the availability of the network specified herein. In all cases, 24/7 access to call center support for issue resolution and assistance is also required.	

2.2 Availability

In order to assure public safety mission critical availability, the following are provided as guidance in meeting the availability requirements that follow:

- Service availability shall not be calculated in such a way as to allow a prolonged outage in one service area to be averaged out in a system wide availability calculation.
- Power backup using battery backup and/or power generators.
- Redundant backhaul circuits from the RAN to the Core and to the base stations.
- High wind loading for the cell towers (TIA 222G requirements for critical facilities or local permitting requirements for critical facilities, whichever is more stringent).
- 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 shall have the ability to take over full operations during a failure or physical loss of a primary operational NOC. Each NOC shall also have redundant network connectivity.
- All redundant components should be regularly tested and operated as defined in the NSA to assure operational readiness in a maintenance window.

Section 2.2 Requirement #	Requirement Description	Additional Information
1	The DBL shall use the appropriate subsets of TL9000 to determine the definition of availability and the method of measuring availability. These subsets, and the definition of availability, shall be negotiated between the PSBL and DBL for the NSA.	The primary resource for measurement and reporting field reliability data is TL9000. TL9000 is an industry standard that covers reporting of network element (NE) outages and field replaceable unit (FRU) failure rates.
2	Public safety requires the ability to use this network for mission critical applications/services.	In order to justify the use of the network for mission critical apps/services, network must exceed the availability of current commercial networks. In public safety's mission critical systems, the availability reaches 99.999%.
3	Availability of the system shall grow incrementally, with the first year service availability being 99.9%, with a requirement of reaching 99.995% service availability at year 10. The DBL shall be required to negotiate with the PSBL to establish a methodology and timeline for achieving these requirements.	This includes disasters, but also doesn't penalize when disaster recovery methods such as emergency deployable systems are successful.

2.3 Access and Control

Section 2.3 Requirement #	Requirement Description	Additional Information
1	The DBL shall enable the PSBL (or its designated entity) 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) should the PSBL choose to do so to manage and operate a separate logical and/or physical database (HLR/HSS/AAA) of public safety user equipment provisioned to use the system. Such access shall be provided in an open format.	

Section 2.3 Requirement #	Requirement Description	Additional Information
3	The DBL shall provide real time access support to the PSBL and public safety entities. Management capabilities include but are not limited to: control, setup, modify user / user group / application priorities profiles, provision/add, manage, and authenticate users and devices.	Real-time access is defined as the ability to make modifications to the user profiles and have those changes implemented. The amount of time between modification and implementation shall be negotiated between the PSBL and DBL, and it is suggested that the value be within 10 seconds.
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. For example, cellular voice services may be obtained through the DBL, and the PSBL may elect to provision users directly into the DBL's Home Location Register (HLR).	
5	The DBL shall provide an over-the-air management framework to PSBL and/or public safety for managing public safety user devices (individually or in groups of devices at one time). 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 monitor the network operation.	
7	The DBL shall inform the PSBL (or a designated entity) of malfunctions or failures that impact service. The time frame for such notifications, the format, and the scenarios in which this information is required shall be established in the NSA. Such notifications shall be provided in a way such that public safety can be notified of such events.	

2.3.1 Notification and Informational

Section 2.3.1 Requirement #	Requirement Description	Additional Information
1	The Public Safety Broadband Licensee and public safety shall 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 negotiate maintenance windows with the DBL. PSBL can also specify exclusion time periods to address major public safety events (planned). Sufficient advance notice shall be provided for these planned activities. Advanced notice requirements shall be specified in the NSA. The PSBL shall coordinate with local public safety entities affected by these activities.	
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.	
3	The DBL shall provide the PSBL (or its designated entity) reports highlighting traffic per public safety user or device such as minutes of use, overall data usage, throughput, and latency. Reports such as Call Detail Records (CDR) or IP Detail Records (IPDR per the IPDR.org published standards) shall be part of these reports. Summary reports shall be provided monthly with the ability to access detailed information electronically more frequently.	
4	The DBL shall provide public safety access to record public safety application/service sessions.	Note that public safety will not likely be able to differentiate personal from work related communications.
5	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. The DBL shall provide the PSBL (or its designated entity) access to this data.	

Section 2.3.1 Requirement #	Requirement Description	Additional Information
6	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. This shall provide a mitigation process for root cause analysis which can reduce future occurrences.	
7	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).	
8	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.	

2.3.2 Hardening Requirements

The public safety community, in stating its requirements for the hardening of communications sites, is looking to satisfy a primary goal:

1. Public safety desires and has a need for a nationwide broadband system to be useful for mission critical communications.

In order to meet this goal, public safety requires that the broadband communications system harden its network with the same level of robustness as current public safety land mobile radio. The public safety community also recognizes that in order to achieve this goal, there will likely be a phased approach to hardening the sites, as an expectation of hardening every site at the beginning is not economically feasible. Thus, the requirements in this section are focused on achieving a network that is better than the current commercial networks, with the expectation that the system will move towards mission critical usage over time. The DBL will be required to negotiate with the PSBL to establish a methodology and timeline for achieving these requirements.

2.3.2.1 Cell Site Hardening Guidance

For disaster recovery and general hardening the PSBL suggest that each cell site and communications center be built to withstand extended power outages and various events affecting cell site to core network communications. The guidelines below are potential solutions that can provide a set of cell site

build standards that would assist in achieving mission critical communications in the event of typical failures or disasters and to deliver the availability specified in this section. In order to deliver on the required availability, an increasing percentage of all cell sites should be fully hardened.

Section 2.3.2.1 Guidance #	Guidance Description	Additional Information
1	The PSBL and the DBL shall agree on a minimum of 4 levels of mobile cell site service criticality levels. CL-1A Primary emergency and disaster response facilities CL-1B Secondary emergency and disaster response facilities CL-2 Targeted Critical infrastructure facilities, staging, or rally locations required for emergency and disaster CL-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	CL-1A sites shall have: 8 hours battery backup power Permanent Generators with 5 to 7 day fuel supply depending on location and accessibility Fully Redundant Backhaul Transmission	Note: redundant backhaul should traverse different Central Offices if applicable. Also note that in areas where land based interconnect is more susceptible to outages (e.g. earthquake or wildfire regions), microwave backhaul is typically used to improve availability.
3	CL-1B sites shall have: 8 hours battery backup power Permanent Generators with 3 day fuel supply Redundant backhaul transmission	
4	CL-2 sites shall have: 8 hours battery backup power Portable Generators with 3 day fuel supply Redundant backhaul transmission	
5	CL-3 sites shall have: 8 hours battery backup power Standardized Connection To Portable Generator Redundant backhaul transmission	

Section 2.3.2.1 Guidance #	Guidance Description	Additional Information
6	If portable generators are used to meet the above requirements, the DBL must demonstrate that they have an adequate number of generators, vehicles to deploy those generators, and personnel trained in the deployment of the generators. Deployment of these generators during regional power outage conditions shall be coordinated with local and regional emergency management and communications coordination bodies to assure system coverage is matching emergency operational needs.	
7	The DBL must provide a generator re-fueling plan that refuels generators prior to exhausting their on-site supplies.	
8	Critical cell sites should 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.	
9	All cell sites should have: Quick connect-disconnect equipment and methods to replace batteries, generator, or fuel storage elements	
10	All cell sites should have: A planned, functioning, survivable re-fueling plan with an annual review and drill exercises program	DBL and PSBL should integrate with public safety disaster recovery plans.
11	All cell sites should have: A planned, functioning, survivable emergency generator deployment and management methodology with an annual review and drill exercise programs	
12	Antenna support structures (lattice towers, monopoles or other structures) should be designed according to ANSI/TIA-222-G (or latest revision), except that the structures shall be designed for a wind speed 15% greater than the Maximum Basic Wind Speed listed in Annex B for the structure's location.	

2.3.2.2 Other and General Hardening Guidance

The following additional guidance is provided to meet the required availability of the network for components and systems other than at individual cell sites.

Section 2.3.2.2 Guidance #	Guidance Description	Additional Information
1	The PSBL and DBL shall provide additional base station hardening, beyond the nominal for that base station, at critical sites identified to provide overlapping coverage (e.g. minimum best server) for a given coverage area. This will be done to ensure that for unplanned/catastrophic outages in the given area, that a subset of the base station infrastructure will be hardened to achieve some nominal system availability.	This will help determine which sites will require what level of hardening per the guidance given in this Section.
2	Operations, Administration, Maintenance, and Provisioning (OAM&P) Robustness: There should 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	Spare core equipment should be warehoused in physically separate buildings away from hazard zones.	
4	Physical diversity should be used for core communications and power. Separate power grids and separate Central Office communications links should be used. Egress and ingress core communications facility entry points shall be at separate locations.	
5	Buildings housing Infrastructure equipment, including at cell locations, should meet or exceed local building codes, fire codes, and safety codes including but not limited to seismic safety standards. Buildings located in coastal locations should be protected from flooding due to a reasonable ocean surge (minimum of 15 feet) for the area.	

2.3.3 Recovery and Restoration

Section 2.3.3 Requirement #	Requirement Description	Additional Information
1	DBL shall address any service affecting outage as follows: • Any instance where 50% or more of the network capacity is affected at the sector level – within two (2) hours • Any other service affecting outage -- within four (4) hours • Any minor alarms within eight (8) hours	Addressing a problem means that the DBL is actively working to correct the problem or is en route to do so.
2	DBL shall need to make available deployable solution for disaster recovery for use by public safety. Beyond disaster recovery and restoration uses, these deployable systems shall be available for deployment in large scale emergency or to isolated area incidents were coverage or capacity of the fixed infrastructure can't meet the operational needs of the incident. Time frame for such deployments shall be specified in the NSA.	Additionally, DBL shall enable other solutions specified in Section 6.
3	DBL must provide customer support at the customer's premises or at an incident in the event of an emergency within two hours of a request for assistance.	
4	The PSBL and DBL shall coordinate in the creation of business continuity plans and disaster recovery plans per NIST SP-800-34.	

2.4 Reliability

Section 2.4 Requirement #	Requirement Description	Additional Information
1	The DBL 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 Telcordia.

Section 2.4 Requirement #	Requirement Description	Additional Information
2	The network operations center owned or contracted for the DBL shall operate on a 24x7x365 basis and shall be required to meet TL-9000 certification in accordance to a mutually agreeable development plan, in no case later than by year 4.	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. The DBL shall coordinate with the PSBL to create the mutually agreeable development plan.
3	The network should offer the capability to do basic self-recovery to expedite service restoration and/or return to redundant operation.	
4	The network 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.	
5	All physical facilities supporting network equipment shall meet contemporary standards for electrical surge suppression, grounding and EMP protection.	At a minimum, the sites constructed for this network should meet standards such as Telcordia/Bellcore to increase the reliability of the sites to withstand electrical anomalies that could render the system inoperable.

2.5 Redundancy

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

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

Base stations that provide overlapping coverage (e.g. minimum best server network design) will provide minimum redundant coverage for that given coverage area.

Section 2.5 Requirement #	Requirement Description	Additional Information
1	The PSBL requires the DBL 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 DBL 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. This gives the DBL the flexibility to restore service by other means.
2	Redundant elements should automatically detect and activate components to provide service upon failures of primary network components.	

2.6 Interfaces and Interoperability[2]

This section provides information regarding interface capabilities and requirements. Implementation of some of these interfaces will be the responsibility of the DBL, while most will be the responsibility of subscribing public safety organizations where the expectation is that the DBL will provide the capability but not the solution. For example, connections to the Internet or other cellular provider networks are common with cellular carries today, thus the DBL would be responsible for these. Examples that public safety will be responsible for include connection to land mobile radio systems, and other public safety VoIP connections.

Section 2.6 Requirement #	Requirement Description	Additional Information
1	The network shall support an interface to Project 25 Inter RF Subsystem Interface (ISSI) Voice Service and Supplementary Services.	Public safety provided.
2	The network shall support an interface to Project 25 Console Subsystem Interface (CSSI) Voice Service and Supplementary Services.	Public safety provided.
3	The network shall support an interface to the Public Switched Telephone Network.	DBL provided.

[2] Note that interfaces that provide an ingress point into the 700MHz broadband network will require robust security controls.

Section 2.6 Requirement #	Requirement Description	Additional Information
4	The network shall support an interface to Integrated Services Digital Network (ISDN) Primary Rate Signaling.	
5	The network shall support an interface to cellular voice networks.	Including but not limited to 3GPP and 3GPP2 networks. This is not a roaming requirement, instead providing telephony calling between the DBL and another cellular provider. DBL provided.
6	The network shall support an interface to IP Multimedia Subsystem (IMS) compliant signaling.	DBL provided.
7	The network shall support an interface to PTT signaling (whether DTMF, PoC, and/or OMA-PoC)	DBL provided.
8	The network shall support an interface to the NIST/OLES VoIP implementation profiles.	Public safety provided.
9	The network shall 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. DBL provided.
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.	DBL provided.

Section 2.6 Requirement #	Requirement Description	Additional Information
13	The network shall support connections between the nationwide broadband network, local area broadband systems and local, state or regional voice and data systems	Public safety provided. Interface mechanisms shall be standardized/open interface solutions.
14	The network shall be interoperable with federal systems and networks to allow connection to authorized federal databases.	Public safety provided.

3 Application/Service Requirements

3.1 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 3.1 Requirement #	Requirement Description	Additional Information
1	Public safety requires that certain applications/services be deployed by the PSBL/DBL. These applications/services are identified in Section 3.2 per the PSBL/DBL column. Other applications/services shall be deployed by public safety via coordination with the PSBL (and per the FCC 2nd R&O).	It is expected that the DBL shall deploy applications/services such as cellular voice and/or push to talk voice. Public safety expects the ability to use such applications/services. Public safety also expects the PSBL to have the ability to deploy its own nationwide applications/services.
2	Public safety shall be able to access both public safety and nationally deployed applications/services simultaneously.	
3	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.
4	Applications/services to be deployed on the network shall require compliance with a test plan.	The test plan shall be developed between public safety and the PSBL for locally deployed applications/services, or a plan developed between the PSBL and the DBL for nationally deployed applications/services.

3.2 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 3.3, the schedule that the application/service shall be deployed, and whether or not the DBL shall 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 3.2 Requirement #	Application/Service	Quality of Service Class[3]	Year 1	Year 4	Year 7	Year 10	PSBL/DBL
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[4]	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[5]	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[6]	3,5	X	X	X	X	
15	VPN traffic	3	X	X	X	X	

Table 3.2 - 1 Application/Service Class Schedule

[3] This column maps directly to the classes of service defined in Section 3.3. Note that QoS Service Class does not imply important, but is instead used to set network performance parameters as defined in Section 3.3.

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

[5] Location and presence information of first responders is highly sensitive data that many agencies feel should be only their control. There MUST be strong controls in place on the data stores such that agencies can control who has access to this information.

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

Application/Service	Description	Data Rate[7]
File transfer	i.e. to download such items as high-resolution images, GIS data, 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[8]
Outdoor video	Outdoor video is video that is transmitted from the street, whether it is surveillance or tactical video.	32-384 kb/s[8]
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, 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

[7] These figures are per application flow. These data rates will be updated over time as public safety's use of broadband matures.

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

Application/Service	Description	Data Rate[7]
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 3.2 - 2 Application/Service Definition and Data Rates

3.3 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 3.3 Requirement #	Requirement Description	Additional Information
1	The network shall 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 shall 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 shall support a QoS class of service for: Transaction data, highly interactive (Signaling)	QoS Class of Service 2
4	The network shall support a QoS class of service for: Transaction data, interactive	QoS Class of Service 3

Section 3.3 Requirement #	Requirement Description	Additional Information
5	The network shall support a QoS class of service for: Low loss, real-time (video)	QoS Class of Service 4
6	The network shall support a QoS class of service for: Low loss only (short transactions, bulk data)	QoS Class of Service 5
7	The network shall support a QoS class of service for: Traditional applications of default IP networks	QoS Class of Service 6

3.4 Network Performance Values for Quality of Service Classes

This section sets the performance values for the classes of service as defined in Section 3.3. This is not an exhaustive set of parameters and values, as each application/service shall 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**[9]						
		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)[10]	150ms	400 ms	150ms	400 ms	400ms – 2s	1 s	U[11]
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 3.5	Section 3.5	U	U	Section 3.5	U	U

3.5 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.

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

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

[11] U means unspecified or unbounded.

4 Security Requirements

The 700MHz public safety network will be used for a wide variety of applications by various public safety organizations. 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 public safety organizations, the network must support a flexible security architecture. Each organization 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 organization.

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 requires 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 organizations or by the PSBL, the following requirements are to be met by the DBL except where otherwise designated.

4.1 Network Requirements

4.1.1 Access Controls

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

4.1.1.1 Device Authentication

Section 4.1.1.1 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 shall 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.	Strong assurance implies resistance to known attacks (e.g. replay).

Section 4.1.1.1 Requirement #	Requirement Description	Additional Information
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.	
3	The device authentication service shall utilize an open standard protocol.	
4	Implementations of the device authentication service 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."	FIPS 140-2 is required pending finalization of the FIPS 140-3 standard.

4.1.1.2 Option to Authenticate User

Section 4.1.1.2 Requirement #	Requirement Description	Additional Information
1	Each public safety organization shall be granted the option to require user authentication in addition to device authentication for certain devices assigned to that organization. When user authentication has been selected as a requirement, the network shall require each of the organization's designated devices to prove its user's identity prior to granting access to network resources	Public safety expects 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).
2	For organizations 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 that provides strong assurance of a user's identity. The DBL shall provide a mechanism to authenticate users against the PSBL password authentication service.	Strong assurance implies resistance to known attacks (e.g. replay).

Section 4.1.1.2 Requirement #	Requirement Description	Additional Information
4	For organizations requiring user authentication, the organization 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 user authentication service shall utilize an open standard protocol.	
6	Implementations of the user authentication service 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."	FIPS 140-2 is required pending finalization of the FIPS 140-3 standard.

4.1.1.3 Authorization

Section 4.1.1.3 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 each public safety organization in coordination with the PSBL.	
2	Each organization shall be granted control over authorization by means of an administrative interface.	

4.1.1.4 Automatic Logoff

Section 4.1.1.4 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).

Section 4.1.1.4 Requirement #	Requirement Description	Additional Information
3	Each public safety organization shall be granted control of the network time-out and inactivity time-out setting for individual devices assigned to that organization.	
4	Each organization shall also be granted via administrative interface the means to manually and forcibly terminate access, including active sessions, to the network for any of its assigned devices individually.	

4.1.2 Transmission Secrecy

Section 4.1.2 Requirement #	Requirement Description	Additional Information
1	The network shall provide cryptographic controls to ensure that transmissions can only be decoded 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 140-2 is required pending finalization of the FIPS 140-3 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.	

4.1.3 Transmission Integrity

Section 4.1.3 Requirement #	Requirement Description	Additional Information
1	The network shall provide cryptographic controls to ensure that received transmissions have not been modified in transit.	

Section 4.1.3 Requirement #	Requirement Description	Additional Information
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.

4.1.4 Audit Controls

Section 4.1.4 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 public safety organization's authorized administrator upon request.	

4.1.5 Availability

Section 4.1.5 Requirement #	Requirement Description	Additional Information
1	The DBL shall make available to public safety organizations, 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 with the latest available plugins).	

4.2 Device Requirements

4.2.1 Access Controls

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

4.2.1.1 Network Authentication

Section 4.2.1.1 Requirement #	Requirement Description	Additional Information
1	Devices shall support the network's device authentication protocol. Each device shall 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.	

4.2.1.2 Option to Authenticate User

Section 4.2.1.2 Requirement #	Requirement Description	Additional Information
1	Each public safety organization shall have the option to require user authentication for device access. When user authentication has been selected as a requirement, the device shall require each user to prove his or her identity prior to granting access to applications or network resources.	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 organization's requirements.

4.2.2 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).

4.2.2.1 Option for Secure Erasure

Section 4.2.2.1 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.	

4.2.2.2 Option to Encrypt Stored Data

Section 4.2.2.2 Requirement #	Requirement Description	Additional Information
1	Devices may support a means of encrypting data stored on the device such that user authentication is required for decryption.	
2	If data encryption is supported, 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 140-2 is required pending finalization of the FIPS 140-3 standard.

4.3 Administrative Requirements

4.3.1 Security Management

Section 4.3.1 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 public safety organizations and users.	Due to the criticality of the network to the safety of the public, the DBL must follow network security best practices (e.g. the protection and isolation of network infrastructure by firewalls).

4.3.2 Designation of Public Safety Authority

Section 4.3.2 Requirement #	Requirement Description	Additional Information
1	Each public safety organization shall designate one or more individuals with authority to exercise the organization's options described in these requirements.	A public safety organization is an entity that subscribes to the public safety network. It may consist of a single agency or a group of agencies that share telecommunication management.
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 or access to any administrative interface	

4.3.3 Oversight

Section 4.3.3 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 public safety.	
2	The findings of any such audit shall be made available to all public safety organizations.	The findings shall be provided upon request via the PSBL.
3	The DBL's security policy shall be made available to all public safety organizations.	The policy shall be provided upon request via the PSBL.

4.3.4 Incident Management

Section 4.3.4 Requirement #	Requirement Description	Additional Information
1	A procedure for managing security breaches or other incidents that may impact the security of the network or public safety organizations shall be developed and documented by the DBL.	

Section 4.3.4 Requirement #	Requirement Description	Additional Information
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 organizations.	

4.3.5 Privacy

Section 4.3.5 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 shall 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 permission is acquired from the subject of the disclosure.	

5 Network Requirements

Section 5 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 75 miles per hour (120 kph).	This handoff scenario is typical for rural and suburban morphologies. Public safety expects the network to be available to all authorized users throughout the nationwide coverage area.
2	The Network configuration shall be documented by the DBL 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. The PSBL in conjunction with public safety shall maintain the right to refuse planned service affecting outages.	An advanced notification period of at least 48 hours prior to the planned outage is required. This will allow the PSBL to notify the affected users. Emergency patches (e.g. virus protection) are an exception but will still require the PSBL to be notified beforehand.
4	The DBL shall establish a joint program to identify Public Safety user requirements affecting the network technology roadmap and support the respective standards development organizations (SDO) processes to make the requirements part of subsequent technology releases.	

5.1 Coverage Morphologies

The following chart describes how the population densities will be calculated into specific morphology classes. These classes will determine each area of coverage, the extent of coverage, data rate and general network performance to be expected within a given morphology class.

- The following morphology classes show in section 5.1 shall be used to determine the classification of a given coverage area. Determinations will be performed via the most current zip code information. Other data sources to aide in the determination may include use of the most current U.S. Census Bureau data.

- The population numbers shown are for the entire populous within a given area and not just public safety users.

Section 5.1 Requirement #	Requirement Description	Additional Information
1	Dense Urban: Population Density +15000 people per square mile And/or (whichever definition meets this criteria) Classified as a business district including: • skyscrapers • high rise apartments • buildings of +20 stories • narrow streets	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.
2	Urban: Population density equal to or greater than 5000 and less than or equal to 14999 people per square mile And/or (whichever definition meets this criteria) Classified as an office/residential district including • hotels • hospitals • buildings of 4 to 19 stories • medium to narrow streets	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	Suburban: Population density equal to or greater than 200 people per square mile and less than or equal to 4999 people per square mile. And/or (whichever definition meets this criteria) Classified as a small business/residential district including: • buildings of 1 to 3 stories • medium width streets	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	Rural: Population density equal to or greater than 0 people per square mile and less than or equal to 199 people per square mile. And/or (whichever definition meets this criteria) Classified as a sparsely populated residential area including: • large open spaces • isolated highways • 1 to 2 story houses • Barns	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	Highway Classified as stretches of interstate highway and/or major highways, principally within rural, extremely under-populated areas.	Problems defining such areas due to issues such as day time population versus night time and other unique situations such as coverage for state highways and major roads shall be handled on a case by case basis between the PSBL and DBL.
6	The defined morphology population densities shall be determined using the most current zip code information.	Other data sources to aide in the determination may include use of the most current U.S. Census Bureau data.

5.1.1 Operational Frequency Range

See FCC 2nd R&O for detailed information.

5.1.2 Minimum RF Requirements

Section 5.1.2 Requirement #	Requirement Description	Additional Information
1	A single common air interface (CAI) shall be utilized for the nationwide 700 MHz broadband network. This CAI shall allow migration to future technology upgrades as determined by the PSBL and DBL.	
2	RAN shall utilize maximum frequency reuse efficiency.	e.g. N=1
3	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 for portable devices.	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

5.1.2.1 RF Interference Requirements

See FCC 2nd R&O for detailed information.

Guidance – The following are recommendations for interference mitigation and not stated requirements.

1) The 700 MHz Nationwide Public safety Broadband Network should be designed to avoid interference to the public safety 700 MHz Narrowband spectrum blocks at 769-775 MHz and 799-805 MHz.

2) The DBL should 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.

3) The DBL and PSBL should create a process to expeditiously resolve interference issues that are identified. The NSA should specify provisions defining responsibility to resolve interference, should it occur, and the level of protection to be provided

5.1.3 Coverage

Section 5.1.3 Requirement #	Requirement Description	Additional Information
1	Network coverage will grow as per the FCC 2nd Report and Order - public safety expects markets to become operational in early 2010 with continual annual coverage enhancements that meet or exceed the FCC requirements.	Specifics on exact markets and timing will be finalized in the NSA.
2	Corridors are defined as major highways and interstates. 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 DBL and PSBL.
3	Coverage areas not officially defined by zip code or census data, such as prisons, park and recreational areas, shall be provided coverage as determined by the PSBL and DBL.	Actual coverage area will be determined on a case by case basis between the DBL and PSBL.

Section 5.1.3 Requirement #	Requirement Description	Additional Information
4	Geographic coverage shall be measured by the DBL each calendar year using capture and data analysis and reporting methods. Coverage areas shall be measured by the appropriate zip code or census data to ensure county, townships, parishes and other similar political subdivisions have 95% of their area covered with 95% availability in that coverage area. (95/95) Actual verification methodology shall be determined in the NSA for both outdoor and indoor coverage and agreed upon by the PSBL.	A annual joint review of the coverage data shall be held between the PSBL and the DBL to determine the extent of PSBL priority user coverage, provide a method to the PSBL to provide input to the DBL for coverage enhancements and expansion, and to enable the PSBL to communicate the availability of coverage to its network priority users.
5	The DBL 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, tall buildings, parking garages and underground.	These areas shall be exempt from in-building penetration requirements.
6	The DBL and PSBL shall make use of industry best practice standards for network design including but not limited to: Minimum best server design.	Minimum best server design helps reduce cell re-selection (e.g. pilot pollution) and ensure the user device can maintain a given data rate for the given signal-to-noise-ratio. Additionally the DBL and PSBL will be able to easily identify sites that provide overlapping coverage and/or critical coverage sites.

Informational: Extended coverage for public safety agencies with aircraft and watercraft will likely be required. This specialized coverage will require coordination and negotiation between public safety agencies, the PSBL and the DBL.

5.2 System and User Coverage, Capacity and Data Rate

These numbers are an average across several technologies and are not meant to specify any one radio access technology.

1) The criteria used for tables can be referenced in Appendix C.

2) These data rates are for outdoor throughput, with an in-building penetration (for network design consideration) that will enable indoor coverage.

3) See requirement 5.1.3 #5 for enhanced indoor coverage

Table 5.2 – 1 Outdoor, single user minimum throughput

The network shall support the following link budget: Morphology	In-Building Penetration Margin	Coverage Availability	Sector Loading Sector is loaded to this level of traffic	Forward Link Throughput • **On street** • **Single user** • Average edge throughput	Reverse Link Throughput • **On street** • **Single user** • Average 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

Table 5.2 – 2 Outdoor, sector aggregate (multiple users) throughput

The network shall support the following link budget: Morphology	In-Building Penetration Margin	Coverage Availability	Sector Loading **Sector is loaded to this level of traffic**	Average Sector Aggregate **Forward Link Throughput**	Average Sector Aggregate `Reverse Link Throughput
Dense Urban	22 dB	95%	70%	5000 kbps	1600 kbps
Urban	19 dB	95%	70%	4600 kbps	1400 kbps
Suburban	13 dB	95%	70%	3700 kbps	1200 kbps
Rural	6 dB	95%	70%	2400 kbps	800 kbps
Highway	6 dB	95%	70%	2400 kbps	800 kbps

Notes:

- On street = “in the clear” (e.g., no additional vehicle or body losses)
- Sector aggregate data rate is for a 5 MHz paired channel (or aggregating multiple sub-channels to 5 MHz bandwidth) and assumes users evenly distributed throughout the coverage area. These figures will significantly increase if using the entire D-Block and PSBL spectrum allocations (20 MHz total). Typical sector throughput and capacity values will vary according to specific site build out, morphology and various other factors and is only meant as a system guideline for capacity.
- Designing a system for the aforementioned outdoor performance will deliver in-building coverage.

In building per user and aggregate throughput rates at the in building penetration margins, loading, and coverage availability specified above will be defined in the NSA.

NOTE: Table above is for first four years of operation. The network should 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 as negotiated between the PSBL and DBL

5.3 Radio Access Network Features

Section 5.3 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 within the DBL network. Handoff/Handover should be seamless to the end user.	This is handoff between sites in the same BSC/RNC versus an adjacent BSC/RNC that is within the DBL network/system. Ensures nationwide coverage if multiple RAN vendors are used.
5	The RAN in general should support a high-data-rate, low-latency and packet-optimized radio-access technology.	

Section 5.3 Requirement #	Requirement Description	Additional Information
6	The system shall support Over the Air Programming (OTAP) for but not limited to terminal configuration updates for new features, security updates, service provisioning, and firmware changes.	
7	By year 4, the network shall support a one way radio access network latency of less than 50 milliseconds.	Latency for this requirement is only for the one way latency of the RAN to or from the mobile station. Actual end to end latency will be determined by the QoS classes as defined in section 3.4.

5.4 Capacity Requirements

5.4.1 Radio Access Network Capacity

Section 5.4.1 Requirement #	Requirement Description	Additional Information
1	The system shall provide the capability to set QoS thresholds for allowed data throughput that 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 shall provide a mechanism to indicate when a user has exceeded the users' maximum monthly data throughput. Public Safety Service should not be cut off. Exceeding the maximum throughput may affect services fees.	Rate capping control mechanisms shall be provided to the PSBL.

5.4.2 IP Core Network Capacity

Section 5.4.2 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)	

5.5 Core Network Features

Section 5.5 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 shall 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 standard network interface drivers that require no user intervention is required in order to connect to the network.	e.g. Support NDIS - Network Driver Interface Specification

Section 5.5 Requirement #	Requirement Description	Additional Information
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 plane, IP transport and mobility management	e.g. “Flat IP architecture”
6	The IP core network shall 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 network shall provide support for routable static IP addressing including the ability to assign static IP addresses to a subset of the subscriber devices employed by Public Safety users of the network.	
8	The PSBL and DBL shall determine IP core implementation that includes but is not limited to: traffic management, peering, determining peering points, IP security / Firewall, Virtual Private Network, Intrusion Prevention, Routing Protocols, Domain Name Service, Dynamic Host Configuration Protocol, Network Management Strategy.	Best practice should be used to avoid single points of failure or at least reduced.

5.6 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. The term secondary user applies to the commercial users, i.e. non public safety.

Section 5.6 Requirement #	Requirement Description	Additional Information
1	The network shall be configured to provide the priority and Quality of Service (Section 5.6.4) 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.

Section 5.6 Requirement #	Requirement Description	Additional Information
2	The Public Safety Broadband Licensee and DBL 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 3.4).	
3	The DBL 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 shall be determined by public safety in coordination with the PSBL/DBL. These user assigned profiles shall be accessible by authorized, designated local administrators.
5	A plan shall be submitted to the PSBL by the DBL for correcting network performance where QoS requirements are not being adequately met.	
6	Public safety users that are in their "home" area shall have a higher priority than users that are not in their "home" area.	

5.6.1 Priority Levels

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

Section 5.6.1 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 shall accommodate priority access to the radio access network and priority access to resources in the core network.	

Section 5.6.1 Requirement #	Requirement Description	Additional Information
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 public safety control.	This allows for public safety control over how an agency assigns priority to users/groups.
5	The DBL shall be able to distinguish between public safety traffic and commercial user traffic.	
6	Public safety requires priority allocation of RAN and Core resources, including (but not limited to) RAN access channels, paging channels, and traffic channels.	This priority allocation shall leverage the same user priority levels used to access the RAN.
7	Public safety shall 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.	

5.6.2 Logging and Records

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

Section 5.6.2 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.	

5.6.3 Limitation of Priority

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

Section 5.6.3 Requirement #	Requirement Description	Additional Information
1	Traffic that exits the 700MHz broadband network cannot be guaranteed to receive priority treatment. Exit in this context means traffic the leaves the network operated by the DBL, such as the PSTN or Internet.	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.	

5.6.4 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 5.6.4 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 3.2.	
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 shall 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.	

Section 5.6.4 Requirement #	Requirement Description	Additional Information
5	The DBL shall maintain a unique user profile for each public safety user or device with all priority levels as assigned by the PSBL. These profiles shall specify the applications/services and QoS levels for applications/service the user or device is authorized for, and the priority level though which that user or device shall communicate	It is suggested that both the DBL and PSBL hold and maintain user profiles to facilitate RAN and core priority schedulers accessing the user profiles for priority treatment.
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 requirements 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 DBL policy and/or the user's profile.

5.6.5 Pre-Emption

This section covers pre-emption from a general perspective.

Section 5.6.5 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 shall not be preempted.

6 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 public safety)

3. Off-network capabilities shall 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 6 Requirement #	Requirement Description	Additional Information
1	The DBL shall enable use of the 700 MHz public safety spectrum for off network communications. This shall 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 shall use up to, but not more than, 3 Watts output power.	
3	D-block licensee shall support PSBL in standards bodies and with subscriber device vendor community to help achieve this requirement.	

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

Appendix A. Glossary/Acronyms[12]

RAN	A Radio Access Network (RAN) 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
PSBL	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
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
FIPS	Federal Information Processing Standard
IPDR	Internet Protocol Detail Record. A usage record according to the format stipulated by the IPDR.org forum.

[12] 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.

NSA	Network Sharing Agreement between the DBL and PSBL in accordance with FCC 07-132.
NOC	Network Operations Center.
OAM&P	Operations, Administration, Maintenance, and Provisioning

Appendix B. References

Federal Communications Commission	FCC 07-132, 2nd Report and Order, August 10, 2007.
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
National Institute of Standards and Technology (NIST)	Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules

National Institute of Standards and Technology (NIST)	800-34, Contingency Planning Guide for Information Technology Systems
International Organization for Standardization (ISO)	ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management

Appendix C. Link Budget Parameters

The table below lists the assumptions used to calculate the link budget. The morphology (in section 5.1) states the "environment" that is under consideration for coverage. Link budget "maps" showing coverage area depend heavily on implementation of a particular 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%		