An Engineering Assessment
# of Select Technical Issues
Raised in the Re-auction of the D Block Spectrum

Prepared for

National Association of Telecommunications
Officers and Advisors
National League of Cities
National Association of Counties
U.S. Conference of Mayors

June 2008

Prepared by
Andrew Afflerbach, Ph.D., P.E.
Director of Engineering

CTC
COMMUNICATIONS
ENGINEERING & ANALYSIS
FOR THE PUBLIC INTEREST

Columbia Telecommunications Corp • 10613 Concord Street • Kensington, MD 20895
301.933.1488 • www.CTCnet.us

Table of Contents

Table of Figures

I. Introduction

This Report presents the results of an engineering evaluation of some of the issues raised by the Second Further Notice of Proposed Rule Making with respect to the D Block of 700 MHz spectrum currently under consideration for re-auction by the Federal Communications Commission.

This Report was prepared in June 2008 by Columbia Telecommunications Corporation (CTC) at the request of the National Association of Telecommunications Officers and Advisors, the National League of Cities, the National Association of Counties, and the U.S. Conference of Mayors.

CTC was requested to prepare an engineering assessment of technical issues underlying the question of how best to structure the D and public safety blocks of spectrum in the 700 MHz band to best serve the goals of deployment of a nation-wide interoperable, broadband, wireless, public safety network. Specifically, this Report:

1. Describes the local input and considerations that will be essential to preserve public safety utility. To successfully facilitate public safety, the model the FCC adopts must enable public safety grade communications as they are traditionally understood, so that first responders and local emergency support workers will make use of and benefit from the network.

2. Describes the need for formalized mechanisms for local decision-making on technical/engineering matters such as interconnectivity with existing local networks and capability to rapidly authorize and de-authorize users.

3. Describes how government public safety and emergency support users must all have access to the network in order for true interoperability to be achieved.

4. Recommends adoption of an immediate skeleton technical standard that will enable pending local efforts to proceed without delay and without risk to interoperability.

5. Describes how any plan that makes joint use of both blocks of spectrum under consideration is advisable from a technical standpoint because the combination of public safety and D Block spectrum enables more efficient use of spectrum and other technical resources. This combined use of spectrum is advisable regardless of business model.

6. Advises selection of a standards-based technology rather than a proprietary technology because such a selection will facilitate both efficiency and competition in hardware vendors -- and will make devices more affordable for both public safety and commercial users.

7. Describes how verification of public safety requirements will be essential because, absent verification, risk exists of mistaken or intentional abrogation of public safety requirements. In particular, testing requirements are essential in an environment in which local public safety has less control than in the traditional public safety communications environment.

II. To Facilitate Public Safety, the Network Must Be Public Safety Grade

The 700 MHz spectrum offers the first opportunity for first responders to use a *public safety-grade* broadband wireless data network, which is far superior for public safety needs (reliability, availability, security) than are commercial grade networks.

This section of this report describes the differences between a public safety grade wireless network and a commercial grade wireless network. It describes why it is critical that the contemplated public safety broadband network be designed and implemented to the public safety standard described above.[1] It also describes the need for local public safety practitioners to have input into design and implementation and sufficient control of their operating environment.

Some first responders do already have wireless broadband devices--in jurisdictions that can afford the recurring costs of such services. As useful as these services are,[2] however, *they are not public safety grade*—they do not run on hardened networks that are designed to withstand certain kinds of disasters—and they may or may not enable public safety prioritization in the event of emergency.

[1] For example, David Boyd, the head of Safecom, a Homeland Security program dedicated to public safety interoperability, has noted that commercial networks cannot withstand the worst of disasters. Mr. Boyd recognized that the private sector doesn't have incentive to build hardened networks that include redundancy and other safeguards—the kind of features that are essential in major emergencies, "exactly when communications is needed most." Government Executive Magazine, "Missed Signals," http://www.govexec.com/features/0206-01/0206-01s2.htm, accessed June 15, 2008.

[2] It is increasingly clear that police, fire, and emergency services responders have growing critical needs for broadband wireless data for such applications as:

- computer assisted dispatching (CAD)
- geographic information systems (GIS)
- incident management tools (such as WebEOC)
- interactive video
- video from live incidents.

A. Comparison between commercial and public safety grade broadband wireless networks

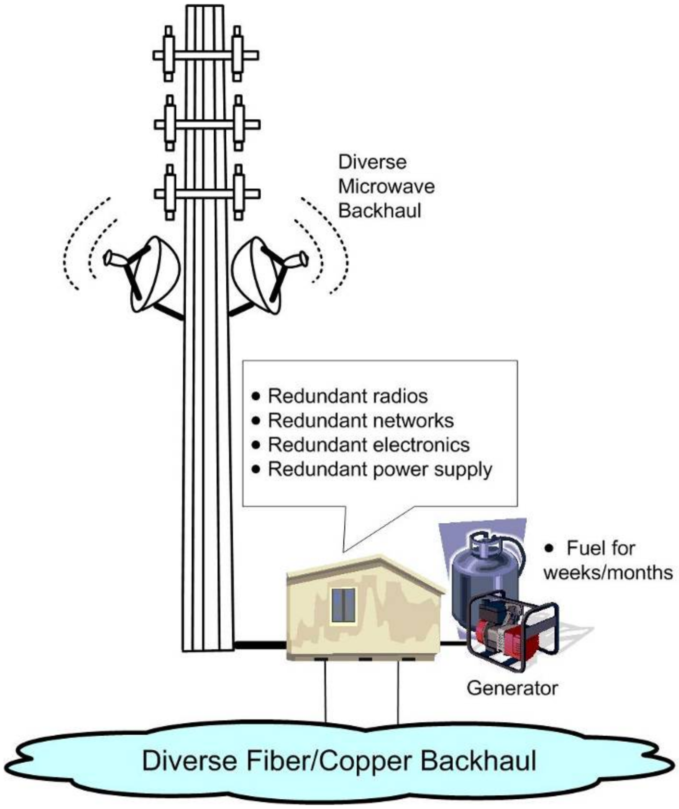
Commercial broadband data networks are designed, built, and operated according to commercial standards of reliability and integrity. There are no formal technical requirements for the performance and reliability of these commercial networks, other than recently adopted FCC requirements for eight hours of backup power at antenna sites. There are no enforceable limits on acceptable outages, guarantees of data rates, or guarantees of performance in emergencies or at the locations of incidents.

Many of the technologies used in commercial data networks have the capability to prioritize certain types of traffic—for example, convey sensitive voice and video applications with higher priority than non-time-critical traffic, such as file transfers. This capability, if implemented, can potentially prioritize public safety applications over others. However, in order for commercial networks to compare to public safety grade networks, the prioritization scheme must keep public safety users on the network in an emergency, even in a scenario where there is extremely high commercial data usage.

In other words, first responders may be no better off than any other user in the event of an incident requiring emergency response—and public safety is therefore compromised relative to use of a network engineered for public safety needs and to public safety standards.

In contrast, a public safety grade network is different in significant respects to a commercial grade network. It is designed with high reliability of the radio signal (availability). It has on-site backup power of weeks or months at all sites. It typically has redundancy of the backhaul connection between an antenna site and the core infrastructure, with multiple fiber, microwave, or copper communications connections. There is redundancy of components at the cell site and at the core. Figure 1 illustrates this general configuration.

Figure 1: Typical Public Safety Network Structure

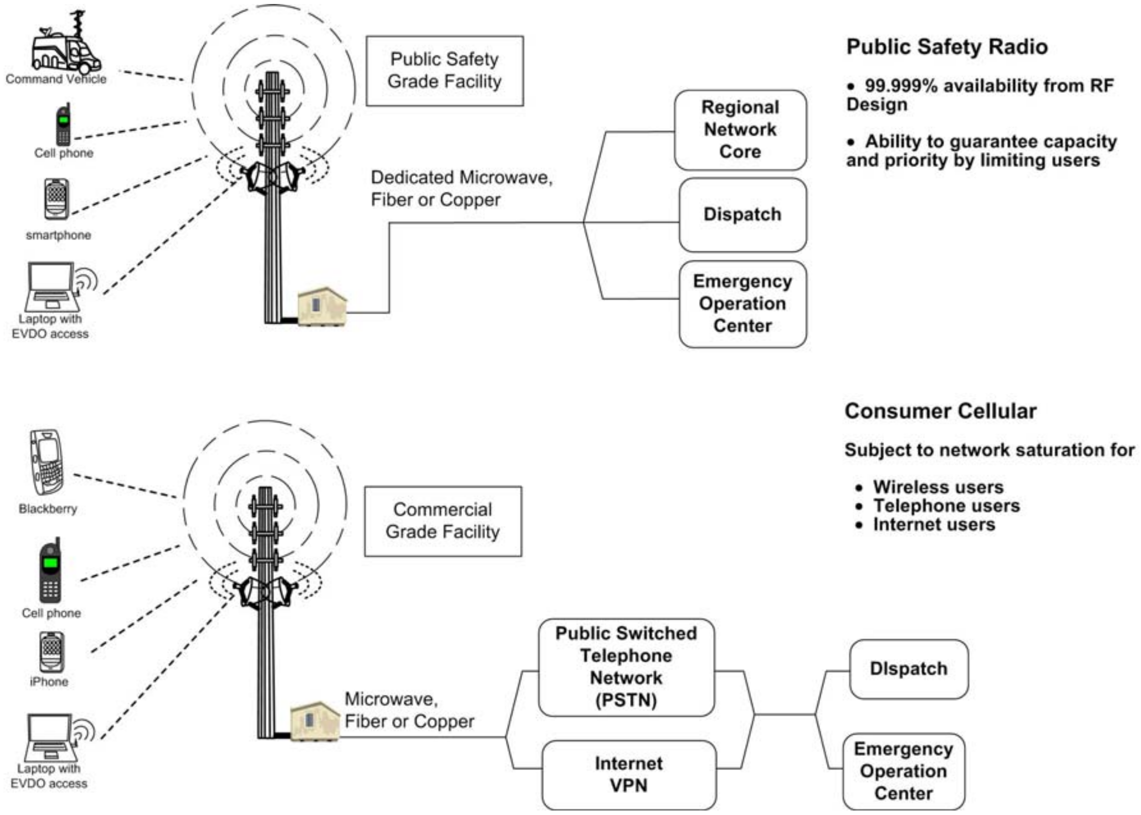


Public safety networks also have the distinguishing characteristic that local government staff performs the following key tasks, all of which help secure the network and maintain its status as public safety grade:

- Determine who has access to the sites and knowledge of the infrastructure.
- Determine how many individuals obtain devices and how they connect to the network.
- Manage capacity usage on the network with a range of techniques, including directly assigning and managing channels and limiting the number of individuals with access to the network.
- Select and authorize all accounts and devices.
- In the event of a security or other event, can immediately disconnect a user or de-authorize a device.
- In the event that a base station or core component fails, the devices at an incident site can “speak” directly with each other in a walkie-talkie mode.

Figure 2 illustrates the contrasting characteristics of public safety grade and commercial grade facilities.

Figure 2: Comparison of Public Safety Grade and Commercial Grade Facility


Command Vehicle
Cell phone
smartphone
Laptop with EVDO access
Public Safety Grade Facility
Dedicated Microwave, Fiber or Copper
Regional Network Core
Dispatch
Emergency Operation Center
Public Safety Radio
• 99.999% availability from RF Design
• Ability to guarantee capacity and priority by limiting users
Blackberry
Cell phone
iPhone
Laptop with EVDO access
Commercial Grade Facility
Microwave, Fiber or Copper
Public Switched Telephone Network (PSTN)
Internet VPN
DIspatch
Emergency Operation Center
Consumer Cellular
Subject to network saturation for
• Wireless users
• Telephone users
• Internet users

Justifiably, first responders do not introduce new technologies or make significant changes in their practices unless the change represents a demonstrable and reliable improvement. If a public safety broadband network does not significantly address the technical limitations of the commercial networks, at least three negative outcomes are likely:

1. First responders will still not have interoperability or a reliable broadband data solution they can use in an emergency, significantly impairing their ability to perform in a critical situation such as 9/11 or Hurricane Katrina.

2. Some localities may choose not to adopt this technology because of its limitations.

3. Even where localities do adopt the technology, many first responders may opt to stay with familiar commercial solutions that they understand and trust, despite their technical limitations.

If, therefore, the nationwide network is to succeed in addressing local public safety needs, the public safety elements of the FCC's original vision should not be diluted.

B. A public safety network requires capacity in any emergency

One of the key limitations of commercial networks is the challenge of adequately prioritizing public safety traffic. There are many technical solutions that identify priority users and ensure that critical communications can proceed in an emergency where networks may be overwhelmed. However, it is critical that the solution that is chosen will address all of the areas that could impact these communications.

A workable prioritization scheme[3] addresses:

1. Ensuring that critical users remain continuously connected even as many critical and non-critical users attempt to use the network and the network becomes saturated.
2. Ensuring that critical users are able to newly connect to the network, regardless of use or saturation and even if non-critical users must be disconnected or limited.
3. Providing sufficient priority to key applications such as voice and video that would suffer in the event of interruption.
4. Enabling critical users to remain connected as they roam from cell to cell.
5. A prioritization scheme among the first responders, so that in the event of saturation by the first responders themselves, the incident commander can prioritize particular applications or particular groups of responders.
6. Sufficient backhaul capacity to support all potential public safety users.
7. Sufficient connectivity to outside resources that users require, such as the Internet, public switched telephone system, and public safety applications and databases

Many of these items are being addressed by Multimedia Prioritization Services (MPS) under development.[4] The existing Wireless Priority Service (WPS) implemented in recent years enables first responders to enter a code to go to the "front of the line" to connect their wireless phones as soon as capacity becomes available.[5] However, this mechanism does not provide any options in the event the cell is already fully used. Moreover, it was designed for voice services and does not extend to broadband data services.

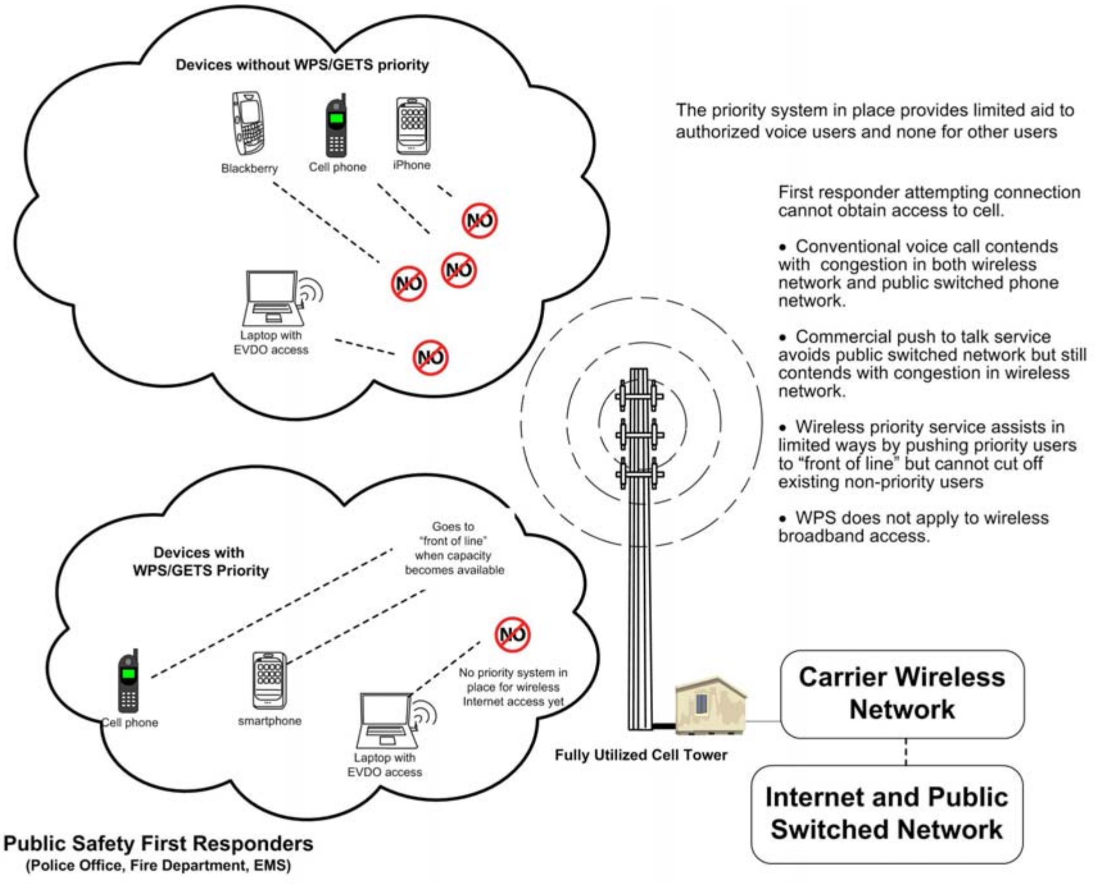
Figure 3 illustrates how WPS works during times of emergency.

[3] "Prioritization" refers to the mechanism to allocate a party of higher priority a higher level of service availability so that their transmissions are given higher priority for continuous connectivity than lower-priority parties.

[4] http://www.3gpp.org/ftp/specs/html-info/22153.htm, accessed June 19, 2008, references a GSM based standard under development; a similar standard is in process for other broadband wireless technologies.

[5] See http://wps.ncs.gov, accessed June 15, 2008

Figure 3: Emergency Scenario at Commercial Wireless Cell


Devices without WPS/GETS priority
Blackberry
Cell phone
iPhone
NO
NO
NO
Laptop with EVDO access
NO
Devices with WPS/GETS Priority
Goes to "front of line" when capacity becomes available
NO
No priority system in place for wireless Internet access yet
Cell phone
smartphone
Laptop with EVDO access
Fully Utilized Cell Tower
Carrier Wireless Network
Internet and Public Switched Network
Public Safety First Responders
(Police Office, Fire Department, EMS)

The priority system in place provides limited aid to authorized voice users and none for other users

First responder attempting connection cannot obtain access to cell.

- Conventional voice call contends with congestion in both wireless network and public switched phone network.
- Commercial push to talk service avoids public switched network but still contends with congestion in wireless network.
- Wireless priority service assists in limited ways by pushing priority users to "front of line" but cannot cut off existing non-priority users
- WPS does not apply to wireless broadband access.

There are multiple technical solutions to provide an acceptable prioritization scheme. One possibility is to dedicate spectrum within the network for the first responders, both for their data usage and in the control signaling for authentication and handoff between cells. Another may be to identify critical users by device and assign their communications a higher priority, provided that the solution has a way to authenticate new critical users, continue operating in a saturated environment, and limit or terminate non-critical communications as necessary.

C. A public safety network requires sufficient capacity and RF coverage

In any event, the FCC's solution must provide sufficient capacity for an emergency first-responder scenario. The requirements depend on the number of responders, the types of application used, and the physical distribution of responders. It also depends on the resources and emergency plans of the first responders

Different jurisdictions and different geographic areas will have different requirements. Moreover, those jurisdictions may need to modify those requirements in an actual emergency, where the geographic distribution may be different from any plan, and out-of-area responders (neighbors, state, federal) may take part. As a result, the network will need to be sufficiently flexible to add capacity in an ad hoc manner.

In any case, designing the capacity in coordination with public safety officials will provide a predictable baseline of capacity and RF coverage. This knowledge baseline is the norm in public safety radio communications. The network may not provide perfect coverage for all conceivable locations, but the limitations of the network will at least be known to practitioners and incorporated into their planning and training. The localities may be able to proactively address limitations of the network through zoning practices and their own augmentation of the network--for example, by requiring owners of large buildings to install amplifiers.

In order to accommodate the capacity requirements, it is recommended that the designers of the public safety broadband wireless network coordinate with local public safety officials to:

1. Design capacity, working with both the day-to-day and disaster scenarios of numbers of users and applications used.
2. Develop an initial service and capacity footprint, with the ability to enhance capacity in later phases of deployment.
3. Determine how additional capacity will be made available in an emergency—for example, by terminating non-critical users.
4. Determine how capacity in particular geographic areas can be enhanced in an emergency, for example, by deploying cells on wheels. Local emergency commanders should be able to own and operate their own mobile cells or call on cells from the operator in a reasonable amount of time.

D. A public safety network must provide access for all government public safety and emergency support users

To best facilitate public safety, use of the spectrum must be extended to all government agencies that provide public safety and emergency support services.

True interoperability includes a wide range of first responders and emergency support functions. In the event of major metropolitan emergency, the first responders include not only fire, police, and emergency managers, but also such emergency support functions as:

- Transportation—to operate and monitor the roads for evacuation and emergency passage
- Public health—to care for and track casualties and casualty movements
- Education—to evacuate or protect students, and to establish shelters for displaced persons

- Information technology—to operate the communications networks, distribute backup radios and other gear, and set-up remote emergency operations centers
- Public works—to secure, protect, and distribute critical water and other resources

It is not only localities that recognize that the integrated nature of emergency response extends to multiple types of responders. The U.S. Department of Homeland Security identifies 15 Emergency Support Functions (ESFs), including not only fire, EMS, and police, but also energy, military, public health, public works, and other agencies that must coordinate responses to emergencies.

E. Because of technological limitations, satellite communications cannot substitute for a terrestrial public safety wireless in the 700 MHz spectrum

Satellite communications provide a significant capability and should be part of any jurisdiction's emergency plans. In a regional emergency where local power, radio towers, and communications utilities are severely compromised (as occurred during and after Hurricane Katrina) satellites may provide the only working technology. There are also portions of the country that are so remote or so distant from significant infrastructure that the only cost-effective and flexible means of communicating is to use satellites. The military is a significant user of satellite technology, and it is one of the only effective ways to flexibly provide capacity in oceans and remote theaters of operations across the world.[6]

It is important to note that satellites have significant limitations as well. Most importantly, capacity in a satellite network is shared by a large potential number of users and may be overwhelmed when a significant fraction of those users needs to access the system at once. Individual satellites fulfill the role of wireless base stations—but while hundreds or thousands of base stations would be built in a terrestrial network, only dozens of satellites would be built in a satellite constellation, placing significant demands on each component of the satellite system. Relative to the terrestrial network, satellite capacity is scarce and expensive.

Because of the limited capacity, satellites must be used more judiciously than capable terrestrial networks. They are limited in their ability to provide images and video.

Because of the delay in signal propagation, some data applications will need to be modified, or may not be effective. Some email applications and services are engineered for short delays and will need to be modified by their programmers not to "time out" over

[6] Maryann Lawlor, "Wideband Global Connection Goes Live," Signal Magazine, Armed Forces Communications and Electronics Association, June 2008, http://www.afcea.org/signal/articles/templates/signal_connections.asp?articleid=1631&zoneid=220, accessed June 18, 2008.

a satellite link. Some multimedia applications will not work effectively when satellite users are delayed relative to other users.

Satellite communications—though essential as a *backup* to terrestrial-based emergency communications systems—cannot *substitute* for a capable terrestrial-based wireless public safety network.

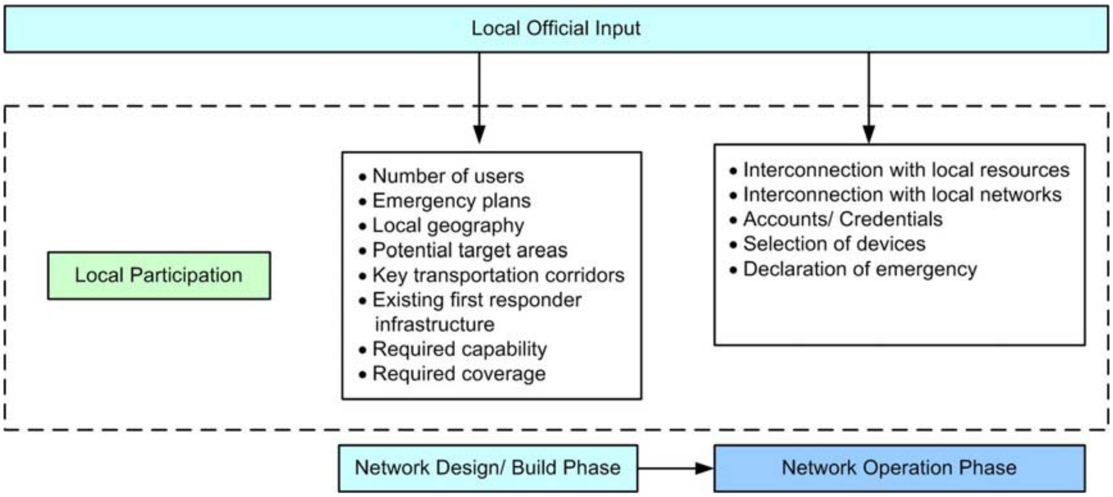
III. There Must be a Mechanism for Local Decision-Making on Technical/ Engineering Matters

Because the vast majority of first responders are local, the designers, implementers, and operators of public safety broadband wireless network should pay close attention to their needs. Moreover, nearly all emergencies are local. Even in national or regional emergencies, almost all communications will terminate within the locality or the state. Although the mission is similar across jurisdictions, the individual departments and jurisdictions vary in scale, density, climate, environment, and internal resources. Urban jurisdictions may have a range of ongoing surveillance requirements and large numbers of mobile staff. Rural areas may have a few individuals covering hundreds of square miles, but may obtain backup from state and local authorities.

Some jurisdictions may have considerable internal expertise and funding and existing network infrastructure. Others may not have funds or expertise or a clear sense of their requirements. In either case, any jurisdiction may be the location of an emergency, and the network must “work” well anywhere.

There should be a well-considered, structured process of incorporating local decision-making and guidance on technical and engineering matters. At the outset of the design process, local first responders must be brought into the process. The designers of the network must work with the requirements of the individual community, including likely number of users, emergency plans, local geography, potential target areas, key transportation corridors, and existing first-responder infrastructure. Figure 4 illustrates two phases of network design/build and network operation.

Figure 4: Phases in Network Design/Build and Network Operation



In the event local jurisdictions have little expertise or infrastructure to contribute, coordination is still necessary to determine the local first responder needs. In that case the network designer may perform the design and implementation using public safety best practices and lessons learned from implementations in comparable jurisdictions.

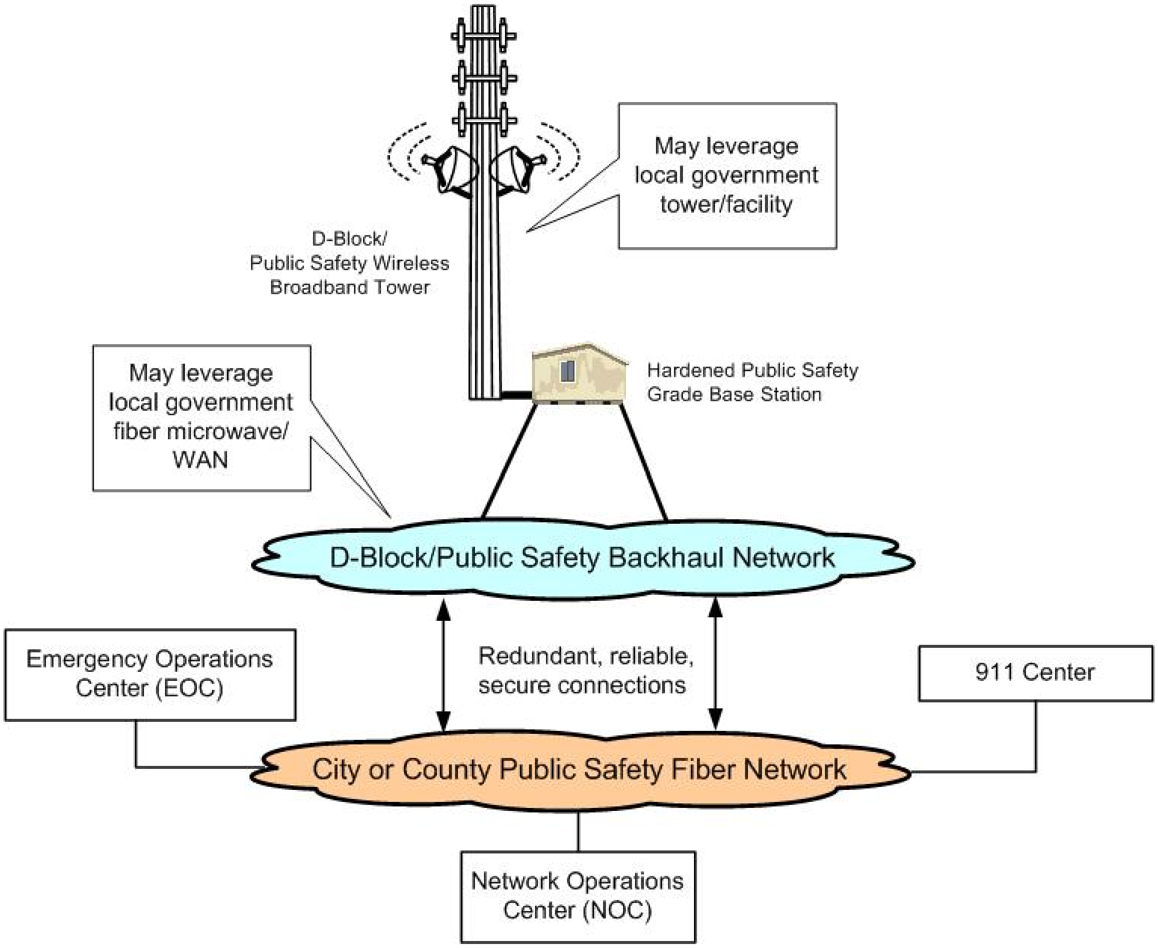
There exists a range of areas that local first responders would need to coordinate to make effective use of the public safety broadband network:

A. Connectivity between the wireless network and the first responder network

The wireless network would require a reliable high capacity trunked connection to the resources of first responders. These include computer assisted dispatching (CAD) and records management systems (RMS), geographic information systems (GIS), file servers, criminal databases, emergency operations centers, local government Internet access, state and federal criminal information networks, national health and hazardous materials databases. The local government networks may include narrowband radio systems, other wireless networks such as WiFi and 4.9 GHz, and local fiber and microwave networks. The connectivity must be sufficiently high-capacity and reliable and use standards-based technologies. It must be secure, so as not to compromise the existing resources or operations. It must be an option for the local community to choose the means of connection; for example, redundant direct connections from the network to a county fiber network that bypasses the public Internet. Conversely, small communities with limited resources should have the ability to make a low-cost connection between its resources and the wireless network, potentially by way of point-to-point wireless connections or leased capacity.

Figure 5 illustrates the public safety grade broadband network facility.

Figure 5: Public Safety Grade Broadband Network Facility

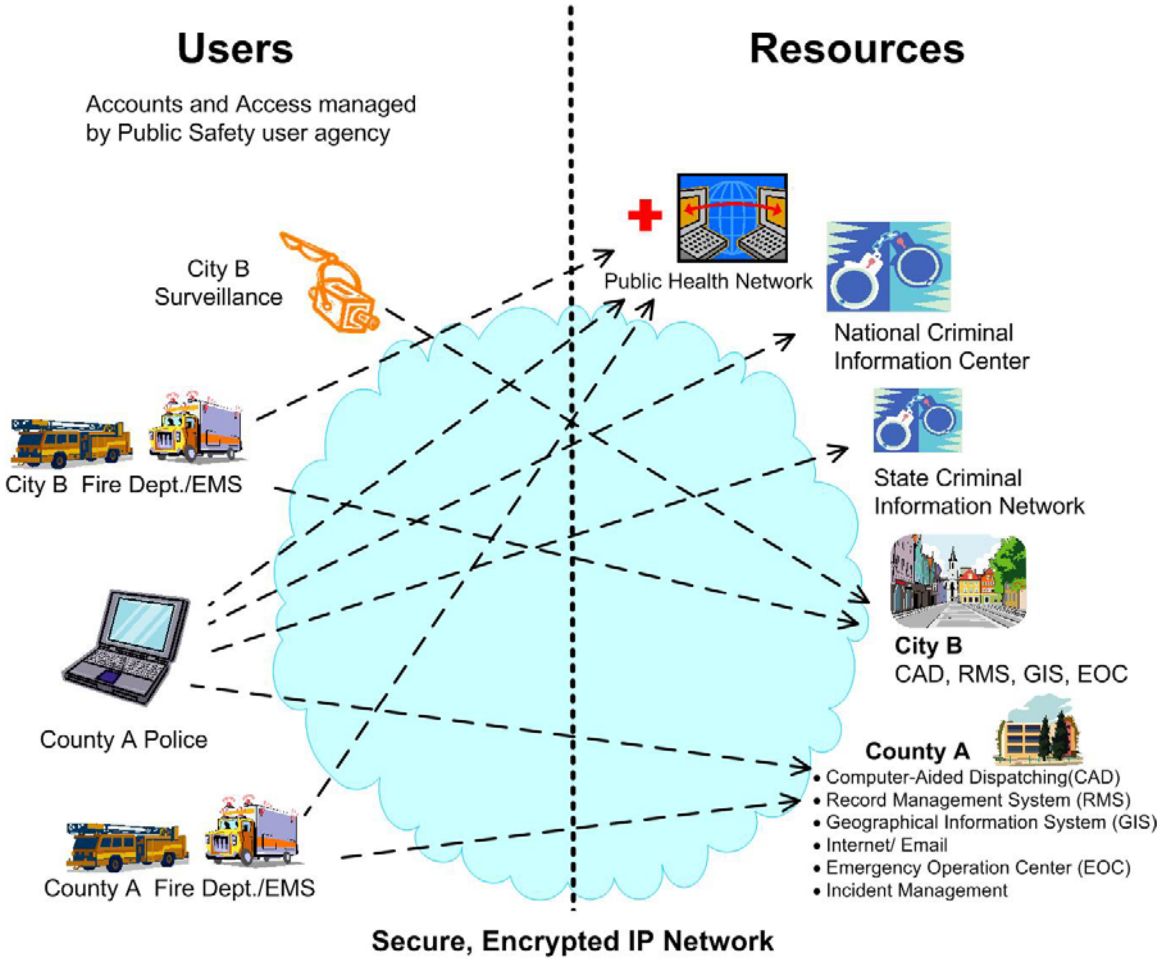

May leverage local government tower/facility
D-Block/ Public Safety Wireless Broadband Tower
May leverage local government fiber microwave/ WAN
Hardened Public Safety Grade Base Station
D-Block/Public Safety Backhaul Network
Emergency Operations Center (EOC)
Redundant, reliable, secure connections
911 Center
City or County Public Safety Fiber Network
Network Operations Center (NOC)

B. *Control of access and authentication and security*

Because the network must be secure, only authorized individuals should be able to use the network as authorized public safety users. There must be strict controls that ensure that unauthorized parties are not able to gain access as public safety users, and that users only have access to resources and networks to which they are authorized. For example, a user from a particular county would be authorized to have access to the network with a particular set of privileges and priorities, and furthermore that individual would be able to reach the authorized resources of that county through the network.

Figure 6 illustrates how users can access shared and dedicated resources over the public safety broadband network.

Figure 6: Utilization of Public Safety Broadband Network


Users
Accounts and Access managed by Public Safety user agency
Resources
City B Surveillance
City B Fire Dept./EMS
County A Police
County A Fire Dept./EMS
Public Health Network
National Criminal Information Center
State Criminal Information Network
City B
CAD, RMS, GIS, EOC
County A
• Computer-Aided Dispatching(CAD)
• Record Management System (RMS)
• Geographical Information System (GIS)
• Internet/ Email
• Emergency Operation Center (EOC)
• Incident Management
Secure, Encrypted IP Network

Local first responders must have the ability to control and modify the network access privileges of all users, because local first responders manage the credentials and privileges of those individuals. This includes account management, the ability to activate and deactivate devices, and the ability to link particular accounts to particular devices. Account changes must be possible 24 hours a day and on demand, such as when a device is stolen or compromised.

C. Local first responder selection of devices

In order to maximize the breadth of innovation and minimize costs, local public safety entities should be able to select any device that meets the technological standard of the network and is certified to comply with the standard and not harm the network. This range of choice is far superior to an environment where the spectrum licensee works only with a particular subset of equipment manufacturers and controls the evolution of the user devices. Desirable examples of technology standards adopted in other areas include WiFi wireless equipment and DOCSIS cable equipment, which are relatively inexpensive and developed by entrepreneurs independent of service providers.

Local public safety entities should be able to select devices based on a range of operational criteria, including their anticipated need (such as mobile data, voice, surveillance), the types of devices they wish to use (such as Personal Data Assistants, rugged radios, laptops, mobile routers), and their existing base of technology (for example, dual-mode 700 MHz/4.9 GHz networks may be desirable if the jurisdiction has a private wireless network).[7] The criterion should be compatibility with the industry standard, so that the relation between the device and the core network is consistent, and the device does not interfere with the operation of the network.

D. Local first responder selection of applications

The public safety network must be able to serve a range of existing and unanticipated public safety challenges. Current public safety applications are known, and others are anticipated for the future. However, other innovations may emerge, and the network must be able to support those capabilities, as long as it is not unreasonably expensive to do so and as long as the new applications do not interfere with other critical applications. For example, innovations in virtual presence or in remote sensing/tracking of people in buildings and concealed areas may lead to developments of new imaging systems that may be transported over the network.

The local public safety entities should be able to determine whether and how to add new applications to the network and should not face exclusions of particular types of communications from the service provider. Where significant increases in usage may unduly affect the other uses and applications, the service provider should work with the public safety entities to determine the potential impact of the application and determine a strategy to implement it, including enhancement to the network and mutually agreed limitations on the use of particular applications.

[7] The 4.9 GHz spectrum refers to that spectrum that has been allocated by the FCC for fixed and mobile wireless services as the designated band for support of public safety. "FCC Designates 4.9 GHz Band For Use in Support of Public Safety and Proposes Licensing and Service Rules," http://www.fcc.gov/Bureaus/Wireless/News_Releases/2002/nrwl0202.html, accessed June 15, 2008. Significantly, however, the spectrum located at 4.9 GHz is far inferior to that at 700 MHz because of the need for line of sight connections. This requires much greater cell density and related network expense. A network in the 4.9 GHz band requires up to 10 times as many nodes as does a 700 MHz network. Telephony Online, "FCC OKs Public Safety Request for 4.9 GHz Mask," http://telephonyonline.com/news/web/telecom_fcc_oks_publicsafety/, accessed June 15, 2008.

E. Local determination of an emergency

In a particular region, the local emergency managers must be able to determine what constitutes an emergency requiring priority use of the public safety network. Almost all emergencies are local, and therefore the local emergency manager should be able to make this determination.

It has been pointed out that all public safety calls represent an emergency to someone, and that potentially the ability to override will result in frequent interruption of commercial users when it is not warranted. At the other extreme is the national Emergency Alert System (formerly Emergency Broadcast System), which enables the President to override all broadcasters and cable systems to speak to the public. It has never been used, not even on September 11, 2001.

To facilitate public safety, the network must work effectively for first responders and save lives. There are routinely emergencies with massive life-affecting local impact (tornadoes, floods, manhunts) that are never known to the nation as a whole. If the local emergency official determines that additional communications spectrum is needed to perform the job, it should be within the latitude of that individual to make the choice without interventional of a state or national official—and without resistance from the D Block licensee.

There may be technological solutions to the problem; for example, a priority scheme that, rather than entirely terminating the commercial use of the spectrum, would instead allocate additional capacity to public safety as needed, perhaps only partially reducing the non-public safety capabilities of the network, depending on the scale of the emergency. Moreover, the geographic reach of the reallocation could be limited to the area where first-responder activity was expected to be most intense.

IV. Expeditious Adoption of Open Standards Will Enable Efficiencies, Cost Savings, and Local Deployment Without Delay--and Without Compromising Interoperability

One of the key ways to make the spectrum useful to public safety users will be to adopt a standardized interoperable technology specification governing key features such as protocols, authentication, and use of channels in the spectrum. Regardless of choice of business plan, the selection of an industry standard will enable jurisdictions and equipment manufacturers to plan network deployments and begin to make interoperable equipment available.

As discussed above, there should be wide latitude in public safety agencies' ability to select devices. However, networks can only be cost-effectively and quickly implemented when there is clarity in the technical standards and in how the network will operate.

Even if there is no single national initiative, the adoption of an industry standard for the spectrum will enable devices to work in any part of the U.S., regardless of how they are managed or financed. First responders and their devices will be able to seamlessly roam to any part of the U.S. It will create a Level 6 Interoperability System according to U.S. Department of Homeland Security standards,[8] immediately creating the highest attainable level of data network interoperability among its users.

Adoption of a technical standard will enable pending local efforts to proceed without delay and without risk to interoperability. It will enable first responders to be prepared in the event of an emergency and enable public safety agencies to begin to migrate from less interoperable, less reliable, commercial networks.

Further, selection of an open standard, with silicon chips and components in common with widely adopted commercial technologies, will keep device costs low. As an illustration, conventional WiFi hotspot access points have fallen from over $500 per unit to $20 per unit in the past eight years of adoption and the sale of tens of millions of devices. In contrast, proprietary public safety push-to-talk radios are manufactured in tens or hundreds of thousands and cost thousands of dollars, despite the fact that they are essentially hardened cellular telephones. Through standardization, devices will become far more affordable for public safety agencies throughout the U.S., a benefit that will also accrue to commercial users.

V. Combined Spectrum Will Boost Spectral and Cost Efficiencies

Keeping 22 MHz of spectrum together is advisable from a technical standpoint, regardless of the business plan selected.

The combination of the spectrum in the public safety broadband and D Block spectrum enables more efficient use of spectrum and other technical resources. There are several reasons why this is a technical benefit:

a. It's a significant advantage to *commercial* D Block customers—they will be receiving services from a public safety grade network that is clearly superior

[8] Level 6 Interoperability is also known as Standards-Based Radio System or "Project 25." It enables over-the-air and wireless communications through shared systems that depend on open standard functionality. Two open air interface standards exist in the US. "Texas Radio Communications Interoperability Plan," Texas Department of Public Safety http://www.txdps.state.tx.us/dem/documents/texasradiocomminteroperabilityplan.doc, accessed June 15 2008.)

to other commercial networks because it was designed to meet first responder needs.

b. Operating a single network in the spectrum will enable a greater body of users to benefit from the antennas, radios, towers, and backhaul systems that will need to be built. If there were separate commercial and public safety networks in the 22 MHz of spectrum, approximately twice the cost of infrastructure would be necessary to make it operate. Efficiency arises from the sharing, by commercial and public safety networks, of a single platform with a single set of antenna structures, base stations, backhaul, management systems, and RF designers.

   If a service provider must build a new network to activate a separate channel band, the cost of the activation may be millions or tens of millions of dollars in a single metropolitan area. Carrier broadband wireless architectures may require base stations every 1.5 kilometers. Individual base station costs vary widely depending on environment and the needs of a particular area, but are on the order of magnitude of $100,000, plus ongoing lease fees. Backhaul costs are significant, with $50,000 to $150,000 required to build a mile of fiber optic cable, or thousands or tens of thousands of dollars per month required to lease comparable capacity from a service provider.

c. A joint buildout will result in less impact to the public rights- of-way because fewer towers, antennas, microwave infrastructure, and/or fiber infrastructure would need to be constructed.

d. Larger spectrum blocks enable operation with large channel bandwidths and high power—making it possible for devices to attain a given speed with fewer towers, each serving a larger area. This type of operation is particularly suitable for blanketing a larger geographic area, as would be necessary to cover rural areas.

e. Larger blocks of spectrum increase the flexibility for serving areas near international borders. King County, WA, for example, has noted the extreme difficulty of operating a wireless network in a major U.S. metropolitan area (Seattle) that adjoins a major Canadian metropolitan area (Vancouver)—and in which each of these networks must share spectrum with the other.

f. If, instead, two adjacent, non-coordinated networks operate in the aggregate 22 MHz, the spectrum allocation will require a guard band between the two allocations, which are currently not separated by a guard band on the assumption that the two blocks will be operated as a whole. Adding a guard band will entail decreasing the allocation of spectrum to the D Block. There will result a greater loss of spectrum use, because of the need for guard bands and mitigation of RF interference among the many individual providers/bands.

VI. Verification of Public Safety Compliance Will Be Essential

The requirement for compliance with public safety requirements of the public/private partnership is literally a matter of life and death. Public safety entities will potentially have much less hands-on control than in their existing networks. There must be a vigorous and transparent mechanism for identifying and enforcing these requirements. It should be made clear in the rules for the spectrum that the FCC will be paying close attention. Either in the rules or early in the development of the network, a penalty level should be determined for missing development milestones, missing deployment deadlines, and failure to meet capacity, coverage, and reliability requirements. There should be a formal mechanism for independently verifying that capacity, coverage, and reliability fulfill the requirements of public safety.

As the network becomes operational, independent testing should continue, as well as enforcement and penalties regarding capacity, coverage, and reliability. There should be regular tests of the prioritization scheme. There should be penalties in the event that traffic prioritization does not operate as required, or in the event that the private partner does not adequately respond to a prioritization request by an authorized official. The security and authentication systems should be regularly tested. User and agency complaints should be logged and reviewed regularly by an oversight entity. Finally, there should be a mechanism for requiring the private partner to address ongoing limitations and problems with the network and perform remedial activity or enhancements as necessary. Absent verification, risk exists of mistaken or intentional abrogation of public safety requirements.