

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
International Comparison and Consumer Survey	)	GN Docket No. 09-47
Requirements in the Broadband Data Improvement Act	)	
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	
Inquiry Concerning the Deployment of Advanced	)	
Telecommunications Capability to All Americans in a	)	
Reasonable and Timely Fashion, and Possible Steps to	)	GN Docket No. 09-137
Accelerate Such Deployment Pursuant to Section 706	)	
of the Telecommunications Act of 1996, as Amended	)	
by the Broadband Data Improvement Act	)	

**COMMENTS OF THE PUBLIC SAFETY SPECTRUM TRUST CORPORATION –  
NBP PUBLIC NOTICE #8**

The Public Safety Spectrum Trust Corporation (“PSST”) hereby submits its Comments in response to the Federal Communications Commission’s (“FCC” or “Commission”) September 28, 2009 Public Notice (“*Notice*”) in the above-referenced proceeding.<sup>1</sup> In the *Notice*, the Commission seeks comment on specific public safety, homeland security, and cybersecurity issues organized into four Categories:

- 1. Public Safety Mobile Wireless Broadband Networks;**
- 2. Next Generation 911 (NG911);**
- 3. Cyber security; and**
- 4. Alerting**

The Comments below focus on Category 1. With respect to Category 2, the PSST believes that a nationwide, interoperable 700 MHz public safety broadband network will be critical to the

---

<sup>1</sup> *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan, Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks – NBP Public Notice #8*, Public Notice, 24 FCC Rcd 12136 (2009) (“*Notice*”).

success of NG911 services. Regarding the more detailed questions in the *Notice* under Category 2, the PSST defers to the Association of Public-Safety Communications Officials-International (“APCO”) and the National Emergency Number Association (NENA), which have more expertise in this topic. The PSST offers no comments on the issues raised under Categories 3 and 4.

**1. Public Safety Mobile Wireless Broadband Networks. One of the issues raised in the Broadband Plan NOI is how to best meet the needs of the public safety community for mobile wireless networks.**

**a. How are public safety agencies making use of broadband networks today?**

Answer: The only practical option for public safety to access broadband today is through the use of the publicly offered 3G commercial networks. Although there are a limited number of other options, such as municipal Wi-Fi (unlicensed) networks or mesh networks, these networks are few and far between. Public safety is accessing the Internet, private networks, and databases using these services where available, but the services lack key features such as mission-critical redundancy, reliability, public safety priority, data security, and wide-area nationwide coverage. They are also generally unavailable in many rural areas.

**b. We seek specific details on both current and anticipated needs of the public safety community for mobile wireless broadband networks and applications. Specifically, we seek comment on:**

- i. the amount of anticipated peak, average, and cell edge broadband traffic and capacity requirements that public safety broadband use is generating and is expected to generate, and the number of current and anticipated public safety users**
- ii. the type of traffic or users’ patterns and usages anticipated for broadband services associated with critical, medium and low demand theater operations**

**Answer:** The PSST can appreciate the desire of the Commission to better understand the broadband needs and requirements of public safety community, but many of the questions asked relative to the anticipated network usage are not currently answerable. As one example, the questions set forth in b.i. and b.ii. above regarding the number of users and other technical questions depend on many assumptions and decisions that public safety would have to make in designing a broadband network. The resources and infrastructure that the potential private partner(s) bring to the network are critical elements for network design. Without knowing who the private partner(s) are and the projected buildout timeframe, it is not practical to make such assumptions.

**iii. applications support requirements and associated data rates for both the down link and uplink operations and associated Quality of Service requirements**

**Answer:** The data rate requirements for public safety are fairly straightforward. The faster the data rates, the better for public safety in the performance of their mission-critical duties. The PSST expects that technology will continue to advance and data rates will continue to improve, which will be very good for public safety. However, past experience with both public safety systems and commercial systems has shown that the demand for services usually grows faster than the speed of improvements in technology. In regards to Quality of Service (“QoS”) issues, public safety needs much higher QoS than what is offered today by commercial services providers.

**iv. current and anticipated public safety device and applications needs**

The following is a list of some of the current and anticipated public safety applications:

**I. Mobile Data Applications**

A. Internet and Intranet access to:

1. Criminal databases for criminal history records and suspect information, including text records and photos of convicted criminals and suspects;
2. Motor vehicle records (drivers' licenses, driving records, drivers' photos, and vehicle info);
3. Nationwide networks like Nlets and the FBI CJIS WAN, and NCIC;
4. Mapping and geographic information systems ("GIS");
5. Records management systems ("RMS");
6. Computer-aided dispatch ("CAD");
7. Receipt and retransmission to responding units of advanced automatic crash notification data;
8. Incident management databases; and
9. Electronic medical records for emergency medical services ("EMS") to retrieve patient medical history from hospital networks and other repository systems

B. High-speed file download and upload, including:

1. Distribution of images, including mug shots and other still photos;
2. Download of critical building floor plan information;
3. Pre-planning and mapping data from a centralized server;
4. EMS multi-vital sign package transmission and remote diagnostics and monitoring; and
5. Continuous multi-vital sign monitoring of multiple firefighters or other responders in structure fires and other hostile environments

C. Real-time asset tracking, including:

1. Tracking of assets, public safety personnel, and resources throughout a region;
2. Automatic vehicle location;
3. Global positioning systems ("GPS"); and
4. Continuous tracking of police, fire, ambulance and other public safety vehicle equipment and supplies on emergency scenes

- D. Text/Messaging/e-mail
  - 1. SMS-like text messaging and e-mail

## **II. Mobile Video and Complex, High-Quality Image Transmission Applications**

- A. Real-time streaming video to command posts and headquarters
- B. Improved situational awareness using video technologies
- C. Ability for dispatchers to distribute surveillance feed videos and on-scene videos to responders and provide a common operating picture
- D. Medical quality video for wireless emergency and community paramedicine (EMS providers assisting in community primary care) applications to enable the supervision of field diagnostic and treatment procedures
- E. Wireless transmission of diagnostic images (*e.g.*, portable computerized tomography and ultrasound images) and video (*e.g.*, ultrasound scanning)

## **III. Mobile Voice Applications**

- A. Public switched telephone network (“PSTN”)
- B. Push-to-talk (“PTT”) voice – one-to-one and one-to-many, like land mobile radio (“LMR”) systems; this application is needed whether or not access to the broadband network is also included
- C. Broadband device access through Internet Protocol (“IP”) gateways to and from public safety LMR systems

- v. **the corresponding extent of broadband infrastructure and backhaul that would be required to support public safety applications, and what technologies and solutions do public safety use or anticipate using to meet these requirements**
- vi. **specific network features and anticipated architecture that will allow the broadband network to operate seamlessly with disaster recovery capabilities nationwide, and the kind of connectivity needed with legacy and other commercial networks**
- vii. **definition and quantification of both mission critical voice and mission critical data**
- viii. **specific requirements for hardening of cell sites and other network facilities, and for other requirements of network survivability and disaster recovery**
- ix. **any studies or other data demonstrating whether and how the requirements needed for urban, suburban, and rural environments currently differ and how they are expected to differ in the future**

**Answer:** The PSST offers no comment on these issues at this time.

- c. **We also seek concrete, itemized data on costs and resources necessary to satisfy public safety broadband needs for mobile wireless services.**

**Answer:** The PSST is not aware of any such concrete data.

- d. **We seek information on experiences and lessons learned to date by current public safety use of mobile wireless broadband networks (whether such networks are commercial or public safety-only), including use of such networks at central locations (e.g., emergency operations centers) and by public safety personnel in the field.**
- e. **We seek comment on what particular mobile wireless broadband needs could be satisfied by commercial broadband service providers in the short term and over the long term. Are there any assessment studies or field trials that show areas in which next generation mobile networks (4G) meet or do not meet Public Safety requirements?**

**Answer:** Next-generation commercial mobile networks (4G) are only beginning to emerge, and the PSST is not aware of any such assessment studies or field trials. Public safety is accessing the Internet, private networks, and databases using these services where available, but the services lack mission-critical redundancy, reliability, public safety priority, data security, and wide-area nationwide coverage. They are also generally unavailable in many rural areas.

- f. **Specific to wireless broadband platforms, what is the expected bandwidth usage for anticipated public safety applications in the short and long term?**
- g. **What actions must the Commission or other entities take to ensure interoperability among public safety broadband systems?**
- h. **We also seek comment on whether public safety users anticipate using a single network for mobile broadband data and voice services in the short or long term, on the obstacles to such convergence, and on how the Commission could help to address these problems or otherwise support efforts at convergence.**

**Answer:** It is not currently feasible for public safety users to use mobile broadband for mission-critical voice service. (See the attached white paper for more information). A long-term vision is difficult and will depend, in part, on the development and availability of broadband technologies that can deliver mission-critical grade voice services. Such

technologies are not currently available or even under development. If such options eventually become available, public safety will need to test them and be convinced that they are mission-critical reliable. In addition, the conversion from traditional LMR mission-critical systems to new technologies will be very expensive, and it will take many years to convert from LMR Voice to Broadband Voice.

Respectfully submitted,



Chief Harlin R. McEwen  
Chairman  
Public Safety Spectrum Trust Corporation  
1101 K Street, NW  
Suite 8100  
Washington, DC 20005  
607-227-1664  
chiefhrm@pubsaf.com

November 12, 2009

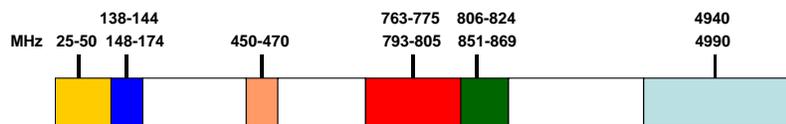
# Public Safety Radio Communications WIRELESS BROADBAND IS NOT AN ALTERNATIVE TO LMR MISSION CRITICAL VOICE SYSTEMS

Chief Harlin R. McEwen  
Chairman, Communications & Technology Committee  
International Association of Chiefs of Police

**There is a misconception by some that in 2-3 years wireless broadband will be an alternative to Land Mobile Radio (LMR) mission critical public safety voice systems. The fact is there are currently no broadband standards being developed or even planned that will allow such an alternative. Current and planned broadband standards and technologies depend on a network approach while public safety must also have a non-network capability to communicate in emergencies when a network cannot be reached or is out of service. This paper briefly discusses the history of public safety radio communications, the proposal to begin using wireless broadband for data sharing purposes, and the danger in assuming that wireless broadband will soon offer an alternative to traditional LMR public safety voice systems.**

Public safety two-way radio communications services have been evolving and constantly changing over the past 50 years. This started with service primarily in the VHF Low Band (30-50 MHz) and then gradually included other spectrum in higher radio bands as public safety personnel needed more radio channels and became more dependent on two-way radio to perform their duties. As a result, the spectrum assigned to public safety in the LMR Service is fragmented and heavily used as there is a limited amount of spectrum available in any one band. Public safety radio services have been limited mostly to voice and low speed data (primarily text messages) that can be delivered on narrowband radio channels. As technology has developed, more and more systems are using digital rather than analog radio equipment. With the advent of digital services public safety has been able to take advantage of new technology and Internet Protocol (IP) applications but digital has also brought new challenges relative to voice clarity and issues related to radio performance in high noise environments.

## Public Safety Land Mobile Radio Spectrum Bands



Allocation	MHz
VHF Low Band (25-50 MHz)	6.3
VHF High Band (138-144/148-174)	3.6
UHF Band (450-470 MHz)	3.7
800 Band (806-821/851-866 MHz)	3.5
800 Band (821-824/866-869 MHz)	6.0
700 Band (763-768/793-798 MHz) <i>Broadband Data</i>	10.0
700 Band (768-769/798-799 MHz) <i>Guardband</i>	2.0
700 Band (769-775/799-805 MHz) <i>Narrowband Voice</i>	12.0
<b>TOTAL .....</b>	<b>47.1</b>

*This does not include 470/512 MHz spectrum used in 11 of the largest US Cities*

4 GHz Band (4940-4990 GHz) 50.0  
*Because of its propagation, this spectrum is only practical for local area networks and hot spots – not for wide area or mobile networks*

In 1995, the Federal Communications Commission (FCC), in concert with the National Telecommunications and Information Administration (NTIA), established the Public Safety Wireless Advisory Committee (PSWAC) to provide an assessment of the communications needs of public safety agencies through the year 2010. On September 11, 1996, PSWAC released a report setting forth the current and future spectrum needs of public safety. Among the findings of the PSWAC report was that 97.5 MHz of new public safety spectrum was needed by 2010, including 25 MHz within five years (i.e., by 2001).

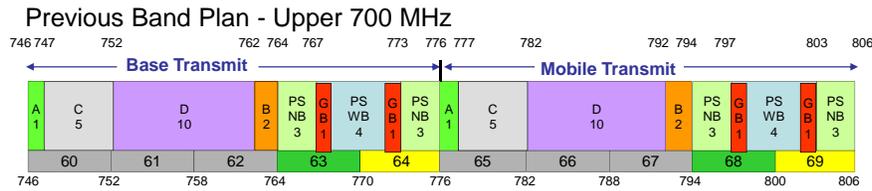
As a result of the PSWAC report, Congress directed the FCC (in the Balanced Budget Act of 1997) to allocate no later than January 1, 1998, 24 MHz of radio spectrum between 746 and 806 MHz (to be recovered from television channels 60-69 as a result of the implementation of digital television). The FCC then reallocated for public safety use television channels 63, 64, 68, and 69. On August 6, 1998, the FCC created the Public Safety National Coordinating Committee (NCC) under the authority of the Federal Advisory Committee Act (FACA). The purpose of the NCC was to recommend rules for the use of the 24 MHz of spectrum in the 700 MHz band.

The NCC, in its final report in July 2003, recommended that half of the new spectrum (12 MHz) be designated for urgently needed public safety narrowband voice channels, and that the remaining 12 MHz be designated for wideband data channels. Since then, significant advances in technology made it desirable for the FCC to convert the wideband data channels to broadband data channels.

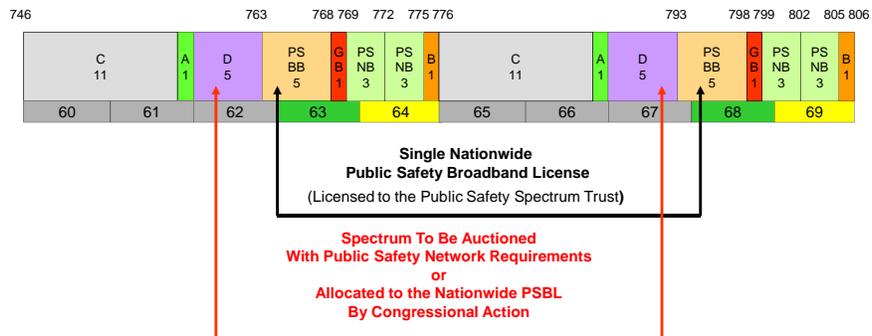
In November 2007, the FCC issued the Public Safety Spectrum Trust (PSST) a nationwide Public Safety Broadband License (PSBL) for 12 MHz of spectrum in the upper 700 MHz band (10 MHz of broadband spectrum and 2 MHz of guardband spectrum). The PSST is a not-for-profit corporation that is organized to hold the nationwide PSBL and to manage the licensed spectrum on behalf of the public safety community. The PSST is governed by a Board of Directors who represent fifteen national public safety organizations, and the PSST has adopted By-Laws that comply with FCC Rules.

Many local and state public safety agencies are implementing or planning locally managed and licensed systems in the 12 MHz of this spectrum that is designated to address the ongoing need for additional mission critical public safety narrowband voice channels. It should be noted that there has been some criticism of the public safety community that they have not used the 700 MHz narrowband voice channels allocated to them in 1997. That criticism is misguided because of the fact that in many areas of the country the 700 MHz spectrum was occupied by TV broadcasters and did not become available for public safety use until the broadcasters were required to move out of that spectrum on June 12, 2009.

On July 31, 2007, the FCC issued the Second Report and Order (Second R&O) that included language which would provide for the holder of the nationwide 700 MHz PSBL (now the PSST) to enter into leases of spectrum usage rights with commercial licensees/operators of the spectrum adjacent to the public safety broadband spectrum (the 700 MHz D Block). The Second R&O included rules for the D Block auction winner(s) to build a nationwide public safety shared wireless broadband network that would be paid for by them and not by the public safety community or the taxpayers. The FCC rules are intended to ensure that public safety will have priority access in emergencies and that the network would be continually refreshed with the latest technical improvements paid for by public safety's commercial partners. Subject to the capacity and other requirements of the public safety community, the Public Safety Broadband Licensee would make the remaining public safety capacity associated with the PSBL broadband spectrum available to the commercial licensees/operators, who would provide the bulk of the financial support for the system through their revenues.



New Band Plan - Adopted by FCC on July 31, 2007



The FCC Second Report and Order also directed that the Public Safety Broadband Licensee would negotiate with the commercial operator(s) to set appropriate rules and technical standards to ensure maximum interoperability, reliability, redundancy, competition, innovation and choices for public safety customers using this spectrum. The network would include a satellite-based element to ensure continuous operations when terrestrial/ground-based equipment is knocked out or in areas where there is no terrestrial service.

The goal is that a Shared Wireless Broadband Network would give public safety:

1. Broadband data services (such as text messaging, photos, diagrams, and streaming video) not currently available in most existing public safety land mobile systems
2. A hardened public safety network with infrastructure built to withstand local natural hazards (tornadoes, hurricanes, earthquakes, floods, etc) that would include strengthened towers and backup power with fuel supplies to withstand long term outages of public power sources
3. Nationwide roaming and interoperability for local, state, and federal public safety agencies (police, fire and EMS) and other emergency services such as transportation, health care, and utilities
4. Access to the Public Switched Telephone Network (PSTN) similar to current commercial cellular services
5. Push-to-talk, one to one and one to many radio capability that would provide a back-up to (but not replace) traditional public safety land mobile mission critical voice systems
6. Access to satellite services to provide reliable nationwide communications where terrestrial services either do not exist or are temporarily out of service

From January 24, 2008 through March 18, 2008, the FCC conducted Auction 73. Almost all of the 700 MHz spectrum, with the exception of the D Block, was sold with the proceeds reaching almost \$20 billion. Although there has been a lot of speculation as to why the D Block was not sold, most in public safety believe it was because the industry had its eye on the unencumbered spectrum that did not include any public safety requirements. On March 20, 2008, the FCC issued an order delaying further D Block action until further notice.

Since April, 2009, several major public safety national organizations have been meeting and have developed a public safety consensus strategy to move this initiative forward. Those public safety organizations believe that there are risks in conducting another D Block auction and the chance of success is better seated in public safety holding the license for the spectrum. On that basis they are moving forward with an effort to get Congress to remove the D Block from auction and to assign it directly to public safety as part of the nationwide PSBL now held by the PSST. This would provide 20 MHz of spectrum within which to build out a nationwide interoperable broadband network.

This would then allow the PSST, through a Request for Proposal (RFP) type process (most likely on a regional basis), to select commercial partners who would partner with the PSST to build out the nationwide network. As part of the nationwide build-out, the public safety consensus group is also advocating that the FCC authorize a mechanism to allow local cities, regions or states to have access to the 20 MHz of broadband spectrum licensed to the PSBL. This will allow local and regional entities to build and maintain their portion of the nationwide network as long as it is interoperable with the nationwide network and allows for nationwide public safety roaming.

On September 24, 2009, a Congressional Hearing was conducted on this topic by the Subcommittee on Communications, Technology and the Internet of the House Committee on Energy and Commerce. Most of those who testified indicated they supported this approach but it was also made clear by one of the witnesses that there are those who are advocating that the D Block be auctioned for commercial purposes without any public safety restrictions.

One issue raised in the Hearing by some Members of Congress were concerns about how much it will cost to build a nationwide public safety broadband network and how it will be funded. Estimates of \$10 billion to \$40 billion have been floated without any real supporting documentation. There is general agreement that if public safety and the private sector can leverage existing private and public infrastructure the cost can be significantly reduced. One commercial company has said that if existing commercial infrastructure was used their cost estimate would be about \$13 billion. Eventual total cost of the network will also be influenced by local build-out decisions. Where local entities or regions want to build out a portion of the national network in their jurisdiction they may each have a different view as to how robust that network should be in their area. While some may be able to take advantage of existing Federal funding programs such as the Urban Area Security Initiative (UASI) Grants, there has been no serious offer on behalf of anyone in Congress to fund this effort. Some commercial companies who have indicated their interest and support for a nationwide public/private network have said it is feasible to fund a nationwide public/private network through the public/private partnerships envisioned. This appears to be the only current option unless Congress were to fund the build-out.

Some of the questions from the House Committee members also indicated a continuing confusion over the 24 MHz of 700 MHz spectrum that was allocated to public safety back in 1997. Some members of Congress and others appear to believe it would be a good idea, rather than allocating the D Block to public safety, to re-allocate for broadband purposes the 12 MHz of spectrum that has been designated for public safety narrowband voice systems. There is a misconception that broadband can replace mission critical public safety voice systems. There are two major concerns with that belief. First, millions of dollars have already been spent in implementing traditional land mobile public safety voice systems in this spectrum and many more are already planned. To stop that progress would be disastrous to the public safety community and the communities they serve. Secondly, and equally as important, is that the claims that in 2-3 years broadband will begin replacing land mobile mission critical voice radio services are based on lack of knowledge of the possibilities to accomplish this.

The fact is there are currently no standards being developed or even planned to provide such a service. The public safety community has endorsed Long Term Evolution (LTE) as the preferred broadband standard for public safety data products and the latest version of that standard (V8) is strictly a data standard that does not include voice capability. The next version (V9) due in late

2010 or early 2011 is planned to include Voice over Internet Protocol (VoIP) capabilities but that version will not have any capability to provide one-to-many communications and talk around (unit to unit) voice necessary for mission critical public safety communications. LTE is a commercial standard that does not recognize the mission critical voice communications needs of public safety. That means that if a first responder cannot reach the network (i.e. a police officer in trouble in a building and his radio unit cannot reach a repeater) or there is no network then the unit is useless. That means no communications and a possible life threatening outcome for the police officer.

It will be many years, if ever, before LMR systems can be replaced entirely by broadband technologies. Before LMR systems could be supplanted, broadband services would first need to be deployed to the level that provides the same extensive coverage that mission critical voice systems provide, including in-building coverage in many instances. Because coverage area decreases as data rate increases, covering the same area at the same level of reliability with broadband services will require even more sites than the number used today for voice communications.

If LTE developers were to eventually develop standards for mission critical broadband voice, the public safety community would need to be involved in the equipment development and would need to see it tested and work in the actual public safety environment on a trial basis before they would be convinced it would be reliable enough to use as an alternative to current LMR narrowband voice systems. System operators and users then would need time to procure and deploy appropriate equipment and devices. The reality of broadband coverage build-out, standards and equipment development, testing in the public safety environment, and follow-on procurement means it would likely be 10 to 15 years or more before most public safety entities would be in a position to seriously consider substituting broadband voice for today's LMR mission critical voice solutions.