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

In the Matter of	)	
	)	FCC 05-80
Spectrum Needs Of	)	WT Docket No. 05-157
Emergency Response Providers	)	
	)	

COMMENTS OF
THE SPECTRUM COALITION FOR PUBLIC SAFETY

Thank you for this opportunity to provide input on this critical public safety issue which our organization was specifically created to address. The Spectrum Coalition for Public Safety ("Spectrum Coalition", "the Coalition") is pleased to offer this "input required for FCC report mandated by the Intelligence Reform and Terrorism Prevention Act of 2004" in response to the "FCC Request(s) (for) Comment On Spectrum Needs Of Emergency Response Providers" ("RFC") in the captioned proceeding, FCC 05-80[1]. The Spectrum Coalition for Public Safety is a non-commercial affiliation of over 30 State, County and Local government public safety communications organizations[2]. Each of our member organizations has responsibility for the

---

[1] *FCC 05-80, "Federal Communications Commission Requests Comment On Spectrum Needs Of Emergency Response Providers, Input Required for FCC Report Mandated by the Intelligence Reform and Terrorism Prevention Act of 2004, WT Docket NO 05-157, (29 March 2002).*

[2] *The Spectrum Coalition for Public Safety consists of the following State, County, and Municipal organizations; Broward County, FL, California Highway Patrol, CapWIN, City of Denver, City of Los Angeles, City of Philadelphia, City of Phoenix, City of San Diego, Fairfax County VA, Los Angeles County Sheriff's Department, Metro Transit Police (WMATA), Montgomery County MD, Region 25 Montana, Rocky Mountain EDACS User Group, San Mateo County CA, State of Arizona, State of Delaware, State of Ohio & Ohio SIEC, State of Oregon SIEC, State of Rhode Island, State of Texas, State of Washington SIEC, U.S Park Police and the District of Columbia. For more information, including an exciting video clip showing how broadband can revolutionize public safety communications,visit the Coalition's website at* www.spectrumcoalition.org .

planning and implementation of the public safety communications systems for their municipalities. The founding Coalition member, the District of Columbia, operates Public Safety Networks, including the Wireless Accelerated Responder Network ("WARN"), a citywide wireless broadband pilot public safety network operating with an experimental license in the 700MHz band. The Spectrum Coalition, therefore, has strong interest in the outcome of this proceeding, and we believe that our comments in light of our experiences in this area will be of value to the FCC.

Reply to Comments

In this response, we have endeavored to provide answers and at least some information for each question posed in the RFC, including as much information from Coalition members directly related to use of spectrum for public safety as possible.

1. Need for a nationwide interoperable broadband network(s): Are our State, County and Local first responders fully equipped to meet the next terrorist attack or even their day-to-day duties? ***No***, in fact today they are not able to use information readily available from their office desk-top computers when deployed in the field. Broadband tools for city-wide remote surveillance, helicopter video transmission, chemical and biological weapons detection, bomb squad support and other uses are critical to preventing attacks and responding to attacks swiftly and effectively to minimize their effects.

Moreover, individual and organizations who wish to do us harm already have access to commercial broadband capabilities in the District, North Carolina, San Diego and elsewhere. They can subscribe anonymously for Verizon or Nextel services across the country and conduct real-time broadband intelligence gathering, video surveillance and, even worse, attack coordination. Our first responders need better tools than the terrorists already have, and this

starts with sufficient spectrum available to support modern, scaleable dedicated and secure broadband wireless networks for public safety. With sufficient spectrum in place, the next step will be to architect a network-of-networks, each with autonomous roaming and that can be configured locally to meet the needs of each municipality.

As the Madrid railway attack makes starkly clear, our first responders need tools to prevent and curtail attacks on our mass transit systems. Wireless broadband networks can quickly support remote sensors that detect biological and chemical weapons at deployment, in time to shut down and evacuate or isolate a rail system before significant casualties occur and/or the problem propagates out of control.

Other broadband wireless tools can help manage those attacks or emergencies that we can't prevent including:

- Real time street monitoring and video pre-assessment capabilities can help first responders and emergency management officials pursue suspects and manage and speed mass evacuations.
- Helicopter video transmission to first responders on the ground and in remote outdoor locations will provide valuable on-scene information from the air, such as video looking down onto burning structures including infrared video providing firefighters with critical hot-spot information to better deal with the incident and to protect firefighter lives.
- On-line medical consultations and pre-admissions assessments during ambulance trips will speed medical care and relieve pressure on hospitals and clinics in the event of mass casualties.

Such capabilities can be utilized to blunt an attack or, better yet, prevent one. We believe that broadband wireless tools are and will continue to be increasingly essential for public safety – and the foundation of these capabilities is the spectrum over which they can be distributed.

2. **Future Public Safety Needs**: Who could have predicted the explosive development of Internet services and its benefits? When we first launched the Spectrum Coalition in March 2003, we had presented and anticipated a handful of broadband applications to justify a 10 MHz allocation in the 700 MHz band. Just over two years later, another half dozen high bandwidth applications either in use or anticipated by public safety have surfaced – and the District's wide-area broadband network has only been in operation since January 2005. The appetite for broadband has far surpassed our expectations and once the broadband foundation exists, its use will skyrocket as has the Internet. Applications currently in use in the District's WARN pilot are only the tip of the iceberg.

Some direction however is clear and certainly the next step will be continuing the evolution towards networks that are standards-based, inexpensive, and that take advantage of the latest technologies. The first responder network of the future should be able to support several levels of users seamlessly any of which can use the network for any combination of video, data, and voice using one device for any and all of these capabilities.

We predict the emergence of a new breed of multi-functional device for public safety that is ruggedized, has a dependable battery system, and will provide every first responder with the voice, text, image, and video information needed to effectively protect life, property, and themselves. These devices would be sufficiently low power to provide a lightweight device that won't further overburden an already heavy load – while providing greater access from the palm of one's hand. They would access criminal databases and provide mugshots, upload fingerprints,

and display Amber alerts. They would relay the location of their comrades and building floorplans for ease of navigation. Finally, they provide immediate biometric information to allow first responders to quickly come to each other's aid in an emergency. They would provide commanders and Chiefs with the needed visual information to allocate the right resources in the timeliest manner. However, these next generation devices can only achieve this high level of capability via broadband wireless connections with dependable wide-area coverage – coverage over vast areas and in the densest of buildings.

Another logical byproduct of the emergence these broadband wireless networks will be the creation of vehicular transceivers to facilitate real-time deployment of Incident Area Network(s) (IAN). Much like vehicular repeaters in public safety voice networks, IANs for broadband data will provide localized in-building coverage and increased local capacity as needed. A similar evolving technology is Personal Area Networks (PANs) where emergency responder vital signs and voice as well as full motion video can be monitored by the on-scene incident commander. These new technologies will bring additional requirements for bandwidth consumption and should be recognized.

Another emerging area of public safety communications is Voice over IP (VoIP). As VoIP continues to gain popularity in the wireline environment, we expect in the 5 to 10 year timeframe this capability to be increasingly desired in the wireless public safety market segment, and is currently being deployed in states served by the Coalition. We believe there is significant value-added by fielding a network that is able to support bundled services for our first responders. These benefits include; reduced varieties of end user devices requiring support, ease of device maintenance, reduction in the quantity of communications devices carried by a first

responder and reduced weight of end user equipment that must continue to be ruggedized when carried by first responders.

3. <u>Should Congress provide an additional allocation of spectrum in the 700 MHz band?</u> We strongly contend that Congress should allocate additional spectrum for public safety communications. Our coalition is concerned that this unique resource be allocated for emergency communications systems to protect the lives and property of citizens. If this spectrum is auctioned it will be gone forever and these five remaining blocks in the 700 MHz bands ("lower A", "lower B", "lower E", "upper C", and "upper D"), are the last spectrum with the desired propagation properties yet broad enough to support the required data speeds.

The demand on a wireless broadband network from one user can range from simple text messaging at 9.6 kilobits per second to multiple real-time streaming video images at over 1.2 megabits per second (Mbps). The District of Columbia has demonstrated[3] that aggregate citywide demand on a network can exceed 50 Mbps and that usage can be concentrated in one area to require 10 Mbps per transmission site – this demand can be placed on a network anywhere, and this level of performance must be delivered throughout the public safety service area. Unfortunately, current public safety spectrum allocations at 700 MHz and 4.9 GHz for wireless data do not meet these needs, as either data speeds do not meet individual and aggregate demand levels or service is limited geographically and first responders must travel to hotspots to secure information – potentially losing critical life-saving time and significantly reducing system utility to the point where the system is, in effect, of little or no value.

---

[3] *A presentation detailing a large-scale event and its aggregate and individual demands placed on a Washington, DC event was delivered to the NCC on February 21, 2003.*

Signal levels at 4.9 GHz degrade far faster than those at 700 MHz consequently delivering a smaller coverage area of a 4.9 GHz base station. Therefore, assuming the deployment of the same technology, complete coverage of a city like Washington, DC would require significantly more sites at 4.9 GHz rather than at 700 MHz. For instance, if we assume free space propagation conditions, all things besides the frequency considered being equal, the range of a 4.9 GHz base station would be seven times smaller than the range of a 700 MHz station. Consequently, citywide coverage would require almost 50 times the number of antenna sites at 4.9 GHz as at 700 MHz. Instead of the 10 transceiver sites required at 700 MHz, 500 sites using 4.9 GHz spectrum would be required leading to significant deployment costs and prohibitive operational costs, and this only to provide citywide coverage *outdoors*.

Actually, these comparisons are optimistic, as they are based on a free-space propagation assumption. In fact, the reality of the mobile propagation environment is worse, and actually worsens for higher frequencies. Significant additional signal losses at the higher frequencies suggest that over 100 *times* more sites would be needed for wireless coverage at 4.9 GHz to match coverage at 700 MHz. In practice, Wi-Fi deployments in metro areas are often quoted as requiring 8-15 access points per square mile, or up to 1,020 access points if all of Washington, DC's 68 square miles were covered[4]. These deployments are at 2.4 GHz, which would typically require significantly fewer sites than a deployment at 4.9 GHz[5] and assume that pole top space is available to accommodate access points – something very difficult to achieve in new residential areas or in large parks. Thus, the 4.9 GHz spectrum is fundamentally limited in reach and

---

[4] *See http://www.tropos.com/support/faq.shtml for Tropos networks quotation.*

[5] *In fact, in the whitepaper "Broadband Public Safety Data Networks in the 4.9 GHz Band,"* (http://www.troposnetworks.com/pdf/Spectrum_Whitepaper.pdf) TROPOS suggests that 2.5 to 4 times the number of sites are required per square mile migrating from 2.4 GHz to 4.9 GHz).

requires numerous repeaters to reach even marginal distances. It is actually best suited to line-of-sight propagation, e.g. rooftop-to-rooftop communications, mesh-type networks where users can create a daisy chain for end-to-end communications, or short-distance communications around a fixed location (hot-spots).

The maximum channel bandwidth in the existing 700 MHz allocation to public safety is 150 kHz. Technologies such as the standardized TIA-902 Scalable Adaptive Modulation have been tailored to this channel bandwidth and offer speeds up to 460 kbps. Unfortunately, this bandwidth does not support multiple video streams for an individual user. Furthermore, the 12 MHz[1][5] of radio spectrum set aside for wideband data must be shared with co-located and adjacent municipalities. In the case of the National Capital Region, the District of Columbia would expect to secure no more than three or four paired channels offering **peak** *citywide* throughput of 1.4 to 1.9 Mbps – far less than projected citywide demand, less than aggregate demand for one transmission site, and less than the peak rates needed by individual users for advanced applications.

We are supportive of a date-certain for DTV transition, because without clearance of the analog television signals, the spectrum will not be available for *any* use.

The DC experience in operating an actual wireless broadband public safety network has highlighted the **need for Congress to allocate more than 10 MHz of spectrum for State, County and Local government**. An analysis of actual network data and the process by which we made this determination is included in a section below.

In addition to this recommended allocation, we also support an additional allocation of spectrum for Federal and public service users. This spectrum should be collocated to promote interoperability, and the needed communications capabilities of our health services, hospitals and critical utilities that are vital to comprehensive homeland security.

4. Can commercial wireless technologies be used for emergency response communications?:

Use of Commercial Wireless *Technologies* for Public Safety: There are significant obvious benefits in reusing as much commercial technology as possible in the deployment of public safety networks – particularly in the areas of cost savings. Benefits to be realized from standards based solutions sharing hardware and applications with commercial offerings include the opportunity for competition in procurement and realization of the economies from volume manufacturing shared with commercial users. Additionally, public safety will benefit from the billions of dollars invested in commercial technologies to enhance their performance and capabilities.

However, these commercial technologies may require some modification to accommodate the public safety environment, such as supporting full ruggedization, enhanced uplink performance, and easily deployed vehicular transceiver systems.

Use of Commercial Wireless *Services* for Public Safety: We are concerned that there would be reliability issues involved with the use of commercial wireless services for public safety communications. Our concerns center on the robustness of commercial network designs, including reliance on UPS with four hour battery lives and single-threaded back-haul networks of leased T1 circuits (with many circuits sharing the same Central Office adding more risk of major single points of failure). Management of these networks in an emergency situation ("event

control”) is not advanced enough to avoid degradation of service resulting from contention for resources during a peak commercial use. Further, design parameters for commercial wireless networks and (private) public safety networks are not based on similar usage models. The customer usage model driving network deployment for commercial service favors downlink traffic over uplink traffic; while the reverse is proving to be the case with WARN.

If public safety were at the mercy of commercial operators for broadband wireless services, it would put public safety at considerable risk. For example, cellular carriers across the country are shutting down Cellular Digital Packet Service (CDPD). The equipment public safety purchased will be obsolete and an expensive change-out is required. Public safety was not consulted on this change - the carriers did this to suit their business interests. In fact, many taxpayer dollars would have been saved if public safety were able to move directly to its own network without implementing alternative solutions. In Washington, DC, the WARN network could have been leveraged. Unfortunately, the District has only an experimental license and can not bring this operational traffic on to the network. Permanent spectrum is then causing significant additional taxpayer expense. Further, the carriers are unwilling to provide detailed performance data to understand where coverage holes exist and public safety must adjust operations to mitigate the effects of inadequate service. While we are pleased with their efforts to address capacity and coverage for planned special events, they are not capable of dynamically addressing unplanned events in the timeframe public safety needs - on the order of minutes. The military wouldn't be willing to take on such risks, and neither should public safety.

There are a number of control issues that are addressed with private dedicated networks including: real-time control of individual user devices, the (re-)configuration of base stations, amount of power allocated to individual users etc. Also, the real-time management capabilities

inherent with a public safety network will allow dynamic reallocation of network resources amongst first responders to best support any specific event and prioritize use of the network on the basis of criticality. This allocation is a complex combination of the bandwidth requirements of all the applications in use on portions of the network serving the incident, the impact of delay on the performance of each application, and the critical need for the application to support the event. This equation changes from incident to incident and needs to be managed dynamically in real-time as each event unfolds.

In the State of Washington, after a major earthquake, there were outages of the public switched network (PSN) and cellular services, while dedicated public safety radio systems provided reliable service. We believe that we need dedicated spectrum because the dedicated systems built on it can be depended upon in times of stress (when most needed by first responders).

In spite of these reservations, we do believe that use of commercial networks has merit. Public safety organizations can partner with commercial service providers, particularly in two areas:

- Use of commercial wireless networks to support roaming when public safety has no coverage and as back-up public safety networks.
- Possibly operation/leaseback of networks built for public safety use by the commercial service providers
    - This would leverage expertise and share costs while maintaining the overall level of control required of a public safety network.

5. <u>Experiences from OCTO's WARN network</u> In the District of Columbia, the Office of the Chief Technology Officer (OCTO) has deployed a twelve site OFDM network to support wireless broadband public safety communications within the District of Columbia. Because this is an IP network, it can more easily support any combination of data, video and voice traffic, and is particularly well equipped to extend any desktop application to deployed first responders.

WARN provides security benefits at several levels. User accounts can be centrally managed where lost/stolen/unauthorized cards can be deactivated rendering them useless (however individual cards can be reactivated if they are recovered). Because WARN is a private network and part of the DC government wide area network, it is intrinsically safer than a commercial network because it is within firewalls, protecting users from hackers and cyber terrorists on the Internet. Using private IP addresses, it is much less vulnerable to security breaches by hackers using techniques like IP spoofing. Likewise, providing service from within a municipalities' wide area network, affords streamlined application deployment users on these networks are trusted.

For a number of reasons, the ability to manage individual user "accounts" enhances the utility of the network for all users. Quality of service can be controlled on an individual user (or user group) basis and we also have the ability to rate cap applications and users as required. This is particularly useful when balancing individual user need and the criticality of individual applications.

Most importantly, the demand for broadband wireless services has far exceeded our expectation. The Washington Metropolitan Transit Authority's Program for Response Operations and Technology Enhancements for Chemical/Biological Terrorism (PROTECT) application frequently clocks over 1.5 Mbps of raw data (excluding IP overhead and control

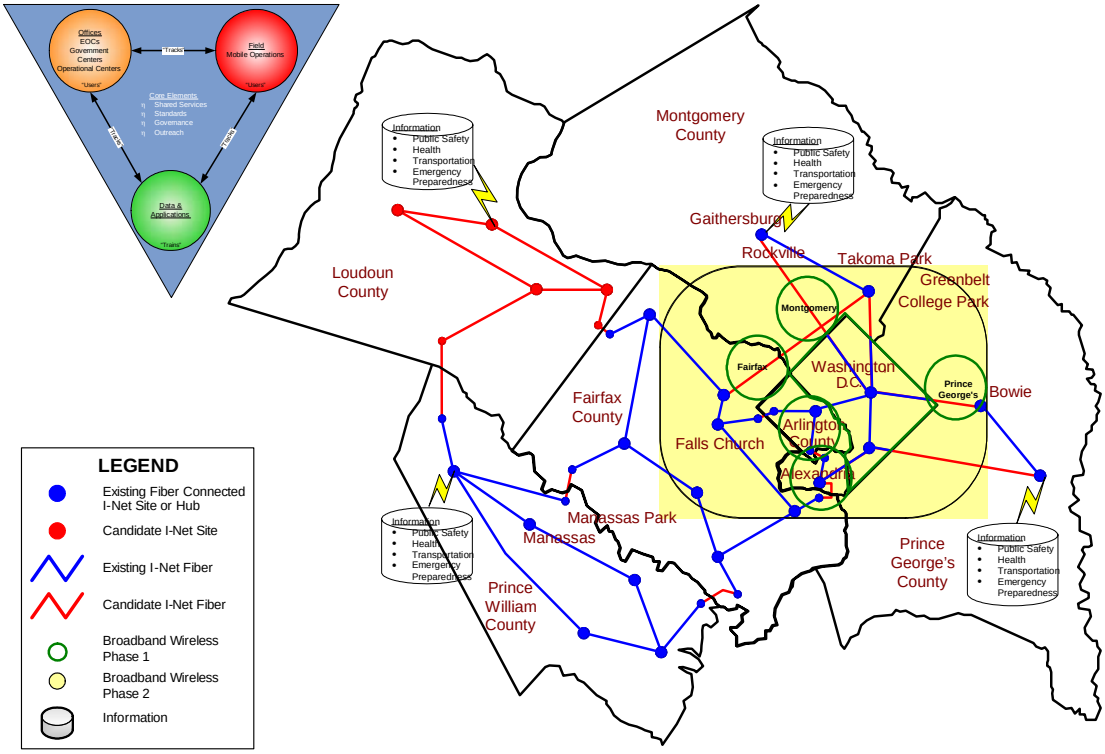
overhead for the air interface). This compares to 1.2 Mbps as originally thought. Further, day-to-day applications such as Computer Aided Dispatch information, such as real-time updates of fleet locations, are needed by most supervisors and updated every 15 seconds to provide the needed immediacy of information. These frequent updates come at the cost of high bandwidth requirements – a peak single user rate of nearly 1200 kbps is not uncommon. This application was not considered in the Spectrum Coalition calculations to arrive at its proposed 10 MHz allocation. Additionally, the quantity of video needed has far surpassed our expectations. Helicopter video is needed not just by the police departments, but also by fire departments. Thermal images transmitted from an overhead helicopter allow firefighters to see where hotspots on the roof may endanger their lives or where fire has spread to another segment.

Finally, we assumed advanced codecs to arrive at 240 kbps for high-quality video transmission. It is true that this throughput can deliver quality MPEG-4 video; however, for various reasons Motion JPG is required and needs far more bandwidth to deliver the needed frame rates. First, Motion JPG is admissible in court, whereas, MPEG-4 is not. Second, Motion JPG can dynamically tolerate various in available bandwidth due to changing RF conditions or network load. As throughput varies for MPEG-4 systems, the images become pixilated and useless. Motion JPG systems degrade gracefully and vary frame rate as throughput diminishes. Unfortunately, Motion JPG systems require far more bandwidth to provide useable "motion." The Washington, DC experience indicates 450 kbps is typically required to deliver three frames per second – where full-motion 30 frames per second is the needed rate.

Initial estimates leading to our 10 MHz proposal did not include additional needs such as vehicular transceivers, airborne subscribers, and unit-to-unit communications. Through the DC pilot network, it is clear that sustaining broadband data connections require much greater signal

levels than do narrowband voice. Smart antenna systems will help mitigate this factor, however, vehicular transceivers are required to deliver both the needed in-building coverage and incident capacity. These vehicular transceivers require an additional frequency in order to operate at peak performance – providing optimal coverage. Helicopters also require broadband wireless communications – receipt of lookout images and the ability to stream high-quality video inexpensively are just a few of their broadband requirements – additional spectrum is needed to accommodate these needs. Finally, no network can handle every scenario. Broadband speeds are needed between units to provide communication where no network coverage exists to allow units to create mesh networks that can connect edge users back to the core network. While this feature is commonly attached to Wi-Fi and similar technologies, it is needed at broadband speeds and at 700 MHz to accommodate public safety missions deep inside buildings. The Governing members of the National Capitol Region have observed the demonstrated value of the District's pilot broadband network and plans have been made to create a regional, fully interoperable, network of networks which will revolutionize public safety data and later voice communications systems. The diagram below provides an architectural overview of this comprehensive network. The initial deployment is being funded by Federal UASI (Urban Areas Security Initiative) investment. Additional investment and more importantly additional permanent 700MHz spectrum is needed to protect our citizens and defend our country.

NCR Interoperability Communications Architecture



CONCLUSION

Public Safety broadband wireless needs exist today and are growing rapidly. These needs far exceed the current commercial capabilities. Dedicated, public safety controlled and operated networks are required. The Washington DC broadband network has proven that that demand has far exceeded expectations. The demand for broadband wireless capabilities for public safety does not stop with State and local agencies. Existing public safety spectrum allocations do not adequately satisfy the demand because they do not address both the throughput and coverage required. Federal agencies require additional broadband wireless capabilities that are available during crises and are interoperable with State and local public safety. The aggregate demand and the ability to meet the demand with current technology far exceeds the previous Spectrum Coalition request for 10 MHz. Therefore, the Spectrum Coalition for Public

Safety recommends that **up to the entire 30 MHz upper 700 MHz block be considered for allocation to Federal, State, and local public safety and the public services they rely on**.

Respectfully submitted,

THE SPECTRUM COALITION FOR PUBLIC SAFETY
441 4th Street, N.W., Suite 707N
Washington, DC 20001
(202)-727-2277

28 April 2005