Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Public Safety, Homeland Security, and	)	GN Docket Nos. 09-47, 09-51 and 09-137
Cybersecurity Elements of a National	)	
Broadband Plan	)	

COMMENTS – NBP Public Notice #8
of the
ASSOCIATION OF PUBLIC-SAFETY COMMUNICATIONS OFFICIALS-INTERNATIONAL, INC. (APCO)

The Association of Public-Safety Communications Officials-International, Inc. ("APCO") hereby submits the following comments in response to the Commission's *Public Notice*, DA 09-2123, released September 28, 2009, regarding public safety, homeland security, and cybersecurity elements of the national broadband plan that the Commission is required to submit to Congress pursuant to the American Recovery and Reinvestment Act of 2009. The focus of these comments will be on questions 1 and 2 in the *Public Notice*, related public safety mobile wireless broadband networks and Next Generation 911 (NG911).

Founded in 1935, APCO is the nation's oldest and largest public safety communications organization. Most APCO members are state or local government employees who manage and operate communications systems for police, fire, emergency medical, forestry conservation, highway maintenance, disaster relief, and other public safety agencies. APCO appears regularly before the Commission on a wide variety of public safety communications issues.

APCO previously filed comments in response to the Commission's initial Notice of Inquiry regarding the national broadband plan and has participated in a variety of proceedings

and forums regarding public safety broadband communications. Unfortunately, the Commission is under a very tight schedule to develop a national plan covering a wide range of telecommunications needs related to "broadband" and, as a result, has been forced repeatedly to seek increasingly detailed information regarding future broadband requirements. However, much of that information is highly speculative, as it necessarily requires estimates of future use of yet-to-be-deployed technologies and applications. In particular, public safety use of wireless broadband services has been limited to date, in part because of the need to rely on commercial networks that often provide insufficient coverage and reliability for mission critical communications.

As request by the Commission, our comments will follow the numbering of the questions in the *Public Notice*. Not all sections or subsections will be addressed due to limitations on time and resources.

1. Public Safety Mobile Wireless Networks

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

Current public safety use of broadband networks is quite limited, and varies across the nation. A small number of agencies have deployed 4.9 GHz systems for limited, short-range broadband applications. The propagation characteristics of the 4.9 GHz band prevent wide-area mobile operation, and therefore the uses now in 4.9 GHz may not be good indications of the potential public safety use of 700 MHz band broadband, which will cover wider areas and be adaptable to mobile use. There are also well-established "wideband" data operations in numerous locations, but they have limited bandwidth and throughput. The District of Columbia's broadband project may provide the best case study of spectrum requirements and

APCO recommends that the Commission seek specific details from the District regarding its experiences and spectrum uses.[1]

Some agencies have also turned to commercial broadband services for certain, mostly non-mission critical, operations as they have no other alternative. Many data applications have not reached "mission critical" status as they have yet to be fully integrated into daily emergency operations. Some applications could easily be considered mission critical based upon content, but users are reluctant to rely upon commercial networks for wireless broadband data in critical emergency situations due to limited coverage, throughput, and reliability. That being said, some commercial networks in some locations are sufficiently robust and may indeed be supporting limited, mission-critical communication in the absence of alternatives. APCO has no specific information regarding those operations.

1(b). Current and anticipated needs of the public safety community for mobile wireless broadband networks and applications

APCO recommends that the Commission examine documentation previously submitted in various dockets that already address many of the issues identified in Section 1.b. In particular, the Commission should consider submissions in PS Docket 06-229 that address public safety requirements for a shared public safety broadband network. Many of the broadband equipment vendors may also be better able than public safety users to address some of the technical issues posed in this section of the *Public Notice*. The following will briefly address a few of the subsections of particular concern to APCO for which information is available.

[1] As discussed at the FCC's Georgetown University field hearing on November 12, 2009, the City of Los Angeles and New York City have also deployed broadband systems, in one case using a commercial carrier for specific types of applications, and the other using 2.4 GHz spectrum, which is not generally available for public safety use.

1(b)(i) Broadband traffic and capacity requirements. The amount of anticipated broadband traffic will be directly related to the size, number and throughput requirements of the anticipated public safety applications operating on the network. The application with the greatest throughput demand today is mobile video. The aggregate throughput impact of voice, desktop extension, internet search, email, CAD, GIS, blueprints, mobile office, sensing, monitoring, AVL, RoIP and many others, along with video, will be substantial and will place tremendous demands on large urban area markets. Traffic and spectrum requirements will increase dramatically for large emergency events on the cell edge where limited capacity and access to a reliable network can be offset with additional base stations and/or available radio spectrum.

The following table was recently provided to APCO and offers a rough estimate of public safety broadband traffic demand. We understand that it is based on data compiled several years ago and may not reflect current projections of application requirements. It is offered for discussion purposes only.

App.	Area Needed	Throughput Per User	Aggregated Throughput	Aggregation Notes
Video	Varies: remote view needs wide area coverage, local view needs incident area view. Incident concentration in one block	100 kbps – 1 Mbps (up and down) depending on video format and quality	Likely 4 – 10 video streams per major incident (400 to 10,000 kbps)	Initially, each public safety vehicle, ultimately personal video.
Imagery (Incident Images, Pictometry	Requires connectivity to central servers from anywhere in the field. Incident can be concentrated in one block.	100 kbps – 1 Mbps (predominately down)	Likely 2-3 per major incident (200 – 3,000 kbps)	Initially, incident commanders, ultimately, all public safety.

Web Browsing	Requires connectivity to central servers from anywhere in the field	20 kbps – 100 kbps (predominately down)	One thousand at dialup speeds requires 30 Mbps	Likely all public safety computers in a municipality will use web applications –
Messaging with file attach.	Requires connectivity to central servers from anywhere in the field	20 kbps – 100 kbps (up and down)	One thousand at dialup speeds requires 30 Mbps	Likely all public safety computers In a municipality will use messaging applications

1(b)(ii). Type of traffic or users' patterns and usages anticipated for broadband services

Broadband communications is expected to become fundamental to public safety communications on both a daily and emergency basis. Robust daily usage applications will include CAD, RoIP, traditional voice, text and data, mobile office and many others. During localized events, such as fires, police surveillance, and EMS responses, broadband requirements will expand with video and other multimedia applications being engaged for inter-agency and intra-agency communications. Major, wide-area emergencies will expand the network usage requirements further to support multimedia communications with local, regional, state and federal users.[2] The specific demands of these low, medium and high usage events will vary from market-to-market and incident-to-incident and have the potential to be very significant depending on the pace, depth and breadth of application adoption.

[2] The District of Columbia Office of the Chief Technology Officer submitted reports to the FCC regarding its 700 MHz broadband experiences using an experimental license during the 2005 presidential inauguration event. We understand that the District's broadband wireless network regularly reached capacity, and that access and capacity per user had to be capped.

1(b)(vii). Definition and quantification of both mission critical voice and mission critical data.

The *Public Notice* seeks a definition and "quantification" of mission critical voice and mission critical data. Whether voice or data communication is "mission critical" is a function of its content and use. Generally, if a significant portion of the communications over a particular network can be essential to an emergency situation, then it needs to operate with mission critical requirements for coverage, reliability, access, capacity, etc. Not all communications within a public safety agency is mission critical (e.g., administrative communication), and the non-mission critical communication can be routed to less robust networks or assigned a lower priority.

Data will increasingly become mission critical as applications are deployed and become integral to public safety operations. While many data transmissions today are probably less "critical" than voice, that is changing as data takes on greater importance in addressing and managing emergency situations.

To the extent that the Commission's question in subsection vii. is meant to address the technical requirements for mission critical communications, those will vary somewhat by network, agency, and the nature of the communications. The most significant work in that regard was completed by NPSTC and the PSST in the Statement of Requirements prepared in anticipation of the D block auction, and addressed by the Commission and other parties to some degree in PS Docket 06-220 and WT Docket 06-150. However, that information was compiled under tight timeframes and in anticipation of a shared commercial/public safety network deployed following an auction. Thus, some of the recommendations necessarily "discounted" mission critical requirements to find the right balance necessary to attract potential commercial

partners through an auction. Time and resources do not allow for a thorough re-examination of those definitions of public safety requirements. What is clear, is that these are issues that the PSST will need to address, working with local agencies regarding their specific requirements, and with private partners where relevant to balance the economic realities.

1(d.) Experiences and lessons learned. There are numerous uses of commercial broadband throughout the country, but these applications are difficult to validate for anticipated 700 MHz public safety broadband since most commercial operators limit throughput and/or charge based on the volume of usage. Throttling back public safety access and throughput during emergency events when the demand is high does not reflect the real public safety operational world. Standard commercial broadband access is already too expensive to promote large scale adoption and if the commercial operator were to provide unlimited throughput and capacity cost models, it would be even further beyond an affordable price point for public safety.

A recent experience on the District of Columbia 700 MHz broadband pilot network that occurred during the 2009 president inauguration highlights the inability of commercial networks alone to provide unrestricted access and throughput supporting critical video and other multi-media applications and requirements. We understand that the commercial carriers were cooperative, but advised the District and other local and federal governments that even with upgrades and temporary cell sites, they anticipated over-congestion on their networks in and around the primary presidential inauguration event areas and venues.

The Regional Broadband Wireless Network (RBWN), a pilot project operated by the District and its partners in the National Capital Region (NCR), became the primary network for the inauguration event in response to the commercial networks' inability to provide the District

and other public safety entities broadband access to support multimedia applications. The RWBN uses the 1x EVDO common air interface, which is also common in commercial networks and a predecessor to the LTE technology selected by public safety. We understand that the pilot RWBN was able to distribute a limited number of access cards to critical first responders and agency command vehicles, and that the system was reliable and successful in facilitating mobile broadband communications throughout the duration of the event.

1(e). Mobile wireless broadband needs that could be satisfied by commercial broadband.

The degree to which commercial services can meet public safety needs has been addressed above in the discussion of mission critical communications. From a technical perspective, commercial services are likely to be able to address *non*-mission critical needs. However, even non-mission critical communications are likely to migrate to more robust public safety broadband networks once they become available. The exception to this may be if commercial services are significantly less expensive and otherwise meet the requirements of the agency in question.

The NOI asks specifically if 4G networks will meet public safety requirements. The preferred 4G technology, LTE, is capable of addressing most public safety *data* requirements (see note below regarding voice). However whether or not a network will handle mission critical communications is a function of the network architecture, not just the technology generation. If a 4G (or any other generation) network is designed, built and maintained to provide sufficient coverage, reliability, capacity, security, etc, then it will likely provide for public safety requirements, assuming the technology has the necessary functionality . The latest and greatest

technology is of little value if it is not available whenever and wherever it might be needed in an emergency situation.

APCO's understanding is that a significant issue with LTE (and other 4G broadband technologies) is that there is no immediate path forward to provide unit-to-unit capability or other essential elements of typical first responder voice communications system.[3] Thus, while LTE will likely offer a voice component, that will not replace mission-critical land mobile radio systems for mission critical voice communications. The voice component will potentially eliminate the need for first responders to carry both a cell phone and a broadband device, but it will not eliminate the need for a first responder to carry a land mobile radio in addition to a broadband device for mission critical communications.[4] In this regard, voice will probably remain the "most" mission-critical communication, as data is unlikely to provide a substitute in life-threatening situations where communication is "rapid fire" and often requires hands-free operation (*e.g.*, at a fire, medical emergency, or crime-in-progress situation). However as noted above, data (including video) is expected to take on greater importance in emergency situations and will quickly assume a mission critical status.

As previously indicated, the District of Columbia may have the most extensive experience with public safety wireless broadband. We understand that during the 2005 presidential inauguration, more than 5 GB were transmitted on the uplink (mainly video from cruisers), and 2.2 GB were transmitted on the downlink over the course of less than 24 hours.[5]

---

[3] *See* Motorola Ex Parte Presentation in PS Docket 06-229 (filed Oct. 28, 2009).

[4] Someday, there may be devices that integrate broadband and LMR operations (*e.g.*, a 700 MHz broadband device that includes 700/800 MHz narrowband radio). Among other potential impediments is battery life. A portable public safety device must be able to operate throughout an 8-10 hour shift without the need to recharge.

[5] The District's broadband network supporting this event was capable of 2.7 Mbps of peak downlink access and 900 kbps uplink per site. That throughout was much less at the cell edge, as was detailed in the District's progress

1(f). Expected bandwidth usage. This section goes to the question of public safety bandwidth requirements. While we will leave it to others to address some of technical aspects of this question, there are at least three critical factors suggesting the need for potential access to 20 MHz of spectrum for public safety broadband: (1) the peak demand in the event of a major emergency, especially in or near heavily populated areas; (2) the importance of having sufficient spectrum to facilitate network sharing agreements through public/private partnerships as a means of funding network deployment; and (3) the efficiencies of using a total of 20 MHz, rather than just 10 MHz, for LTE.

The City of New York and others have indicated that they believe public safety could require as much as 20 MHz for broadband, at least on a peak demand basis. For most areas, 20 MHz is probably more than will be required in "normal" circumstances. However, demand will fluctuate over time periods, which is why a shared public/private network would be the most efficient use of the spectrum as it would allow commercial users to benefit from spectrum capacity that would otherwise be underutilized in the absence of an emergency. Importantly, 10 MHz alone would not be sufficient to justify a shared network as there would be relatively little excess capacity in most areas most of the time.[6]

Finally, a 10 MHz + 10 MHz paired allocation (total of 20 MHz) would provide for more cost-efficient spectrum use. With LTE, the system infrastructure necessary for a 5 MHz + 5 MHz system is be similar to that required for a 10 MHz + 10 MHz system. In other words, for roughly the same cost, you can provide twice the capacity. Furthermore, without adding spectrum, the only way to increase capacity may be to add sites, which greatly increases network

---

reports to the FCC. Future capacity requirements are likely to be even greater, especially with anticipated application enhancements (*e.g.*, MPEG 4 video).

[6] *See* comments submitted by PSST and other parties on this point in WT Docket 06-150 and PS Docket 06-229.

construction and operational costs. APCO understands there to be other spectral efficiencies with a 10 MHz + 10 MHz allocation for broadband, and urges the Commission to seek the technical details from the appropriate vendors if such information is not already in a record.[7]

1(g). Interoperability among broadband systems. Interoperability issues for public safety broadband have been addressed in this and other proceedings (see in particular comments in PS Docket 06-229 regarding petitions for waiver).[8] Interoperability requires a common technology standard, and public safety entities have been unanimous in their support of LTE. Additional interoperability issues related to LTE have been examined by the Broadband Task Force.

1(h). *Convergence of broadband voice and data*. As discussed above, we anticipate that initial broadband deployments will be primarily for data, perhaps with a voice component, but not for mission critical voice in most situations. The current technical limitations of 4G technologies to provide required voice communication functionality for first responders (*i.e.*, unit-to-unit), and initial coverage limitations, are likely to prevent full convergence of all public safety voice and data communications until far into the future, if ever.

2. Next Generation 911

2(a). Broadband infrastructure requirements. Many operational requirements for the delivery of multimedia, data and voice over IP are being stated by the public safety community but supporting data to identify specific bandwidth needs are either several years old or not yet

[7] APCO understands that Motorola and perhaps others will be addressing this issue in presentations at the FCC's field hearing on November 12, 2009, at Georgetown University (the same day as the due date for these comments).

[8] *See* Comments of APCO (Sept. 22, 2009) and other comments filed on or about October 16, 2009.

available at the national level. There are regions that have engaged independent firms to analyze potential requirements but this data has not been compiled recently in a useful format that would provide a definitive scope for the FCC. It is known that broadband must be capable of handling IPv4 and IPv6 packet transmissions.

2(b). Status of NG911 technical standards. The technical standards for NG911 will be provided within several documents being produced by either NENA or APCO/NENA jointly. The Detailed Functional and Interface specifications, referred to as "i3", are scheduled for industry release in the first quarter of 2010. In addition to NG911 standards, the ATIS Emergency Services Interconnect Forum (ESIF) will be releasing technical interface standards for the IP selective call routing transition environment, during which many PSAPs will employ a combination of legacy and NG911 technologies. This standard referred to as the "RFAI" is scheduled for industry release in the first quarter of 2010.[9]

c. Current deployment of NG911 and near-NG911 technologies and services. There are a number of IP capable systems deployed as well as elements such as text and vehicle telematics. It is not on a large scale and none are being used in the context of "near NG911" as of yet. A driving factor in these deployments has been the need to accommodate non-verbal communication such as text and multimedia for special needs populations and for consumers who have come to rely on these forms of communication. PSAPs in areas facing financial challenges, but who also must replace legacy equipment that is no longer maintainable, are

[9] There are many devices that will be associated with NG911 for the purpose of call routing, location verification, and border control functions. None of these devices are currently deployed in public safety. Many devices are still in development.

seeing value in pursuing IP-based equipment and emergency service network implementation rather than face the need to upgrade again when NG911 deployment becomes more common.

2(d). Regulatory roadblocks that may be restricting more vigorous NG 911 deployment? Regulatory changes will likely be needed at both the federal and state levels. However, it may be premature to identify those changes until there is further development in the technology and standards.

2 (e). Automatic location identification in the NG911 environment to facilitate. NG911 location acquisition will be handled via LoST (Location to Service Translation) servers in conjunction with other servers that validate addresses, enforce routing policies and control ESInet access (border control functions). These technologies, as stated above, are in development. The obvious advantage to PSAPs will be the ability to receive a more accurate location from Internet based 911 calls. Whatever technology becomes the standard(s), care must be taken not to lose any more of the benefits of traditional landline-based location information. The deployment of wireless communications led to reductions in accuracy and other E9-1-1capabilities. Similar results must be avoided in future technology transitions.

CONCLUSION

APCO hopes that the information in these and other comments being submitted to the Commission will be helpful in the development of the National Broadband Plan and in other related proceedings.

Respectfully submitted,

/s/

Robert M. Gurss
Director, Legal & Government Affairs
APCO International
1426 Prince Street
Alexandria, VA 22314
(571) 312-4400, Ext 7008

November 12, 2009