



City of Phoenix

TO: FCC, PSHSB

FROM: City of Phoenix, Phoenix Arizona

RE: ADDITIONAL COMMENT SOUGHT ON PUBLIC SAFETY, HOMELAND SECURITY, AND CYBERSECURITY ELEMENTS OF NATIONAL BROADBAND PLAN

NBP Public Notice # 8

Also Referencing: GN Docket Nos. 09-47, 09-51, 09-137, PS Docket Nos. 06-229, 07-100, 07-114, WT Docket No. 06-150, CC Docket No. 94-102, WC Docket No. 05-196

Comment Date: November 10, 2009

Introduction:

The City of Phoenix is responding to the FCC PSHSB request for current and future broadband needs by providing information for select questions in this notice. The City views the potential opportunity to access and participate in the development of a public safety grade broadband network as a benefit to the public, along with a clear opportunity for commercial network providers to also participate, profitably.

The City of Phoenix Public Safety Departments (Police and Fire) provide support to many other communities through IGA or Regional Governance agreements. These agreements in one form or another depend on the reliability of commercial broadband networks for cooperative interoperability. This interoperability extends to almost 3000 square miles from the center of Phoenix. Indirect interoperability extends throughout the State of Arizona and beyond.

Review of Opening Comments in Notice:

Broadband offers a variety of potential benefits to emergency responders and other public safety agencies. However, commenters in the record have noted that these networks may not meet specialized public safety requirements. Public safety agencies today typically have only access to broadband services that they obtain from commercial service providers. In particular, public safety agencies generally lack access to mobile wireless broadband service that meets their specialized requirements (e.g., coverage, hardening, reliability, etc.). If such broadband capability were made available to public safety, for example, it could allow firefighters to receive a recent video of a fire scene or perhaps blueprints or understand where hazardous material is located even as they proceed to the fire scene or police officers to receive videos of a crime scene or an accident or even a suspect or evidence. Further, improved broadband services could enhance the public's ability to call for help in emergencies and public safety's ability to provide warnings, alerts, and emergency information to Americans in times of emergency or need. However, achieving these potential public safety benefits also requires consideration of how to implement and maintain a broadband infrastructure that is resilient in the face of cyber attacks and similar threats to network security. Accordingly, we seek additional comment on the following specific issues to help us better understand these issues as we develop a National Broadband Plan.

Response from the City of Phoenix:

We mostly agree with this general view of commercially available broadband services. The City of Phoenix has utilized commercial wireless data services that have been available since CDPD was offered. Commercial services and infrastructure have been significantly cheaper to use and much more reliable, adaptable and available than any infrastructure or equipment marketed by “public safety” communications equipment providers. The Phoenix Fire Department, since adapting a technology path using commercial wireless services, has always been able to track technology improvements and try to be able to provide “information, anytime, anywhere”. Private infrastructure technologies utilized by the Fire and Police Departments, for the majority of its wireless information delivery, has typically become obsolete before physical failures begin, unsupported by manufacturers and developers, and has been very costly and difficult to replace. Replacement systems are not available, due to spectrum limitations, which compare in reliability, cost or coverage potential that any private, affordable, infrastructure manufacturers can provide.

While commercial broadband services have been available a majority of the time to us and reliable enough to utilize for daily public safety communications (voice and data), we still experience brief periods of failure, due to the lack of an ability to obtain a quality of service level agreement and some level of oversight on how the systems are designed or maintained. Outage periods have been experienced that last 1 or 2 days, that have either a minor or major impact.

Open common “protocol” broadband services are highly desirable for the City of Phoenix that are conditioned for the reliable public service needs.

Requested Information Sought:

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?*

- The City of Phoenix is using broadband networks today to provide connectivity between Computer Aided Dispatch systems, Records Management Systems and National Database Information systems to obtain/provide time sensitive dispatch information, location/accountability information, pictures, maps, videos and other commercial device enabled capabilities from fixed computers, mobile computers, and handheld devices. The greatest amount of voice traffic generally not involving life safety situations is also carried by these broadband networks, 24hours a day, 7 days a week. These networks provide the ability to send a receive information to public safety members not only locally (3000 square mile area) but nationally and internationally. The same networks also enable technical staff to resolve internal problems quickly, without needing to respond to a specific location to gain access to our internal networks.

The City of Phoenix has provided VPN and other internet accesses to internal information that are much more accessible when utilized over these same broadband commercial networks.

All future dispatch and information systems that are being planned at this time by public safety members within the City of Phoenix are intended to be designed to be compatible with commercial standard broadband devices and networks. This will allow the City to operate as cost effectively as possible by utilizing common equipment and standards rather than unique technologies that are not massed produced or sufficiently tracking technology improvement trends.

- 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

- Broadband traffic is very difficult to measure, as this information would need to include all devices that are currently utilizing the variety of broadband networks that are now utilized and the number of different devices that are being used. Public Safety (Police and Fire) will frequently update maps and files that may be as large as 40 or more Gigabytes, to almost 3000 vehicles. Commercial broadband networks today can not handle this type of traffic without a significant impairment to them, so fixed locations are established. The inability to not be able to provide this type of information in a genuine mobile environment, as quickly as possible, frequently causes a delay in obtaining updates about locations or “bad guys”, to help insure the safety of our public safety responders as quickly as events or incidents occur or change.

ii. the type of traffic or users’ patterns and usages anticipated for broadband services associated with critical, medium and low demand theater operations

- Typical peak activity for heavy-traffic broadband would be scheduled generally during times when there is less response activity. This is harder and harder to find as our City and adjacent partner areas in Maricopa, Pinal, and Yavapai Counties do not have as many quiet periods as once existed 20 years ago. It would be preferable if broadband access and our heaviest data could become available through mobile delivery rather than having to depend upon fixed point locations. But, this only describes a single type of large data support needs. During other types of peak activities, we are very dependent upon these same commercial providers to support us with sufficient bandwidth for “cell phones”, picture and video transmission for personal devices, etc. these type of events are usually very isolated (Super Bowl, 4 Alarm fire, Special Police Incident) in which we are not the only users of this same network and always compete for shared use with members of the public and media.

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

- This again will always vary. Public Safety users within the City and in partnership with the City (19 other Fire Departments). What can be anticipated is that with every change that is made with a personal or commercial device, is that that will become what the next level will be needed and developed by our commercial partners. Our applications are always modified or updated based on the dynamics of the industry. It is the preference of the City that a QOS is established as a part of any Public Safety broadband effort. This will not only help to identify what we can expect at best, but at the same time allow any commercial network developers identify the minimum technology and staffing necessary to be able to maintain that level of need. It is understood that QOS is only a number, but it is at least a common reference point in which all can work from and plan around under normal circumstances.

iv. current and anticipated public safety device and applications needs

- The largest demand now and in the future for responding public safety users will continue to be mobility (personal and mobile computer) and those applications that are used in that environment.

- 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*
- We are in need of infrastructure that provides reliable connectivity for over 3000 square miles, and growing.
 - 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*
- At this time, we would not be dependent upon a public safety broadband network provider to also provide our connectivity to commercial networks. This would be enabled through our own systems. Additionally, a public safety network should not be internally designed so tightly and restrictive, that interconnectivity with other systems would be limited or impossible. The network should be as open as possible and allow the end users / governance bodies to control the security levels.
 - vii. *definition and quantification of both mission critical voice and mission critical data*
- This will always be defined by the personal communication devices supported by the broadband networks. In addition, it would be preferential to also be able to develop mission critical voice communication systems that are not available in the form of a personal device at this time. Self-healing mesh network technologies are dependent upon a broadband network for operation. This type of design can provide a significant improvement to all voice communications used today on narrowband spectrum. The future narrowbanding of public safety voice communication systems will be at a cost in reliability, audio quality, and in some cases, safety. Broadband networks and devices that are now being used have the potential ability to reverse many of the bad effects being felt by public safety users of voice communication systems. Broadband networks could enable voice communications to levels never before available using FM audio or other digital encoding methods to date, by improving dynamic range, audio conditioning, and true tonal quality of voice and background sounds.
 - viii. *specific requirements for hardening of cell sites and other network facilities, and for other requirements of network survivability and disaster recovery*
- The sites should be hardened from vandalism, have 8 hour redundant power systems, hot standby and multi path microwave (or fiber) network connectivity. These should also be designed to withstand historical weather patterns for the area.
 - 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*
- Within the Phoenix and adjacent areas that we support, it has been very typical that if there is a need as a rural area now, 10 years from now it will most likely be an urban need. A

planning and designs should anticipate rapid growth and unexpected high levels of demand, due to any incident that may happen to occur within that area and require higher than normal levels of public safety support.

- c. *We also seek concrete, itemized data on costs and resources necessary to satisfy public safety broadband needs for mobile wireless services.*
- To date, the majority of services that are obtained from existing networks are fixed costs of \$40 - \$50 / month, per user. We are not privileged to always know what resources are provided, for that cost and are not possible to always know without a QOS agreement.
- 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.*
- The best experience we have is failure of these networks. This has allowed us to develop all of our devices and applications anticipating the eventual failure and lack of accessibility. We are not at all dependent on these systems for daily operation, but take full advantage of them for enhancing our ability to serve the public. A public safety grade broadband network may allow us to change these parameters, but it has been proven to us to never be dependent on only one path/network for providing critical information.
- 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?*
- A very large majority of public safety's needs are being provided by commercial providers already. Voice, data, video, location, etc. As the commercial networks expand their capability, we try and track this with technology refreshment of our devices, when fiscally possible.
- f. *Specific to wireless broadband platforms, what is the expected bandwidth usage for anticipated public safety applications in the short and long term?*
- We would always anticipate using the highest levels available for brief periods of time and then very small bandwidth needed during a majority of the time. Mostly daily needs are very bursty, short, messages that access internally available data information or are made available through "browser" applications.
- g. *What actions must the Commission or other entities take to ensure interoperability among public safety broadband systems?*
- Regional governance is the best approach to determine how interoperability should be achieved. Not all networks can or should be designed the same in each area of the country as not all applications, practices, or policies are the same at a technical or operational level. There is much greater success in the development of pockets of infrastructure managed and used under a regional governance model.
- 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.

- No. It has been shown that we cannot depend on any single network design. Even if a public safety grade network were built and deployed nationally, we would utilize any other commercial networks that may be available for, at least, redundancy.
2. **Next Generation 911 (NG911).** The Broadband Plan NOI has also been exploring whether the American public could use broadband technologies to better communicate with emergency responders when they make 9-1-1 calls.
- (No Comments at this time)
3. **Cyber security.** Another important issue the Broadband Plan NOI has been examining the survivability of broadband networks and cyber security.
- a. *What type of computer-based attacks against government or commercial computer systems or networks (i.e. cyber attacks) are occurring or are anticipated to occur, and what are other federal agencies, commercial, and other entities doing to prevent, detect and respond to cyber attacks?*
 - (No comment)
 - b. *How are other federal agencies of the United States and other governments collaborating with the communications segment to prevent, detect, and respond to cyber attacks?*
 - (No comment)
 - c. *What market incentives exist for commercial communications providers, large and small, to invest in secure infrastructure? (i.e., how do we avoid externalities?)*
 - This should be able to provide a much more marketable product for corporations, if the network design utilizes common standards acceptable by the majority.
 - d. *Do end-users have sufficient independent information to make good decisions between communications providers that may differ in the extent to which they implement cyber security measures?*
 - No. It is incumbent upon the end user to insure end-to-end security at this time. Dependency upon a commercial provider without a QOS is a mistaken decision.
 - e. *How widely are cyber security best practices implemented by communications providers and what are these best practices?*
 - Any network built should be able to clearly articulate how they have achieved best practice status.
 - f. *What are the specific wireless network features and handset features and capabilities necessary to combat such attacks?*

- (No comment)

4. Alerting.

- a. *To what extent are broadband technologies currently being used as part of public emergency alert and warning systems? Please provide specific descriptions of their use as part of these systems, including system capabilities and limitations and examples of jurisdictions where such systems are currently in use.*
- The City of Phoenix currently maintains a Community Emergency Notification System. As more and more members of the public and sworn members of public safety abandon the use of wireline services for direct communications access and are only using broadband communication devices, broadband service reliability and accessibility for the City is now more necessary than ever before. The City does not currently have any ability at this time, through the use of commercial wireless providers, to be able to prioritize the accessibility needs of its regional community. While this is very rarely needed in our region, it is most likely a common need in many others.
- b. *How can broadband technologies improve the effectiveness of emergency alerts for all Americans, including people with disabilities, people living in rural areas and people who do not speak English? Comments should include information on improvements to message content, geographic targeting, system security, and speed of message transmission from the alert initiating government agency to the public.*
- With the many adaptable technologies that are available today and the availability of a public safety grade broadband network, public safety emergency alert information can be customized for each individual, if appropriate information is available about that individual. Currently, dependency upon mass-dialing systems through wired technologies is slow and not always reliable. By adapting commonly used communication tools (email, SMS text messages, etc.) and allowing members of the public to select their own personal form of notifications and in whatever language may be available through a commercial translation service.

This information was compiled from response by several employees within the City of Phoenix or is a contact for further information:

Phoenix Fire Department
Deputy Chief Leif Anderson, Division Chief Doug Mummert, Ron Burch, Mark S. Schroeder
150 S. 12th Street
Phoenix, AZ 85034

Phoenix Police Department
Gary Avery, Lori Rhyons
620 W. Washington
Phoenix, AZ 85003

Phoenix ITS / RWC
Bill Phillips
149 N. 4th Ave, 2nd Floor
Phoenix, AZ 85003

Response Contact Information:
Mark S. Schroeder
Office: 602-361-7286
mark.schroeder@phoenix.gov