Federal Communications Commission
Notice of Inquiry: National Broadband Plan for Our Future
GN Docket No. 09-51
(Sections 72-79, 115, pages 26-29, 38)

III. DISCUSSION

F. Specific Policy Goals of the National Broadband Plan

3. Public Safety and Homeland Security

General Comments:

- There is some merit to a nationwide broadband network, but there needs to be some flexibility for jurisdictions to build out early
- Due to forthcoming narrowbanding requirements, jurisdictions are forced to look at abandoning their current legacy mobile data systems and look at commercial carriers to provide a wireless transport mechanism
- Using commercial carriers – which do not provide priority to emergency services – is risky
- A standard should be developed by the PSST and jurisdictions should have the opportunity to build out to those standards immediately

Section	
72	***In the development of a national broadband plan, the Recovery Act requires that the Commission include "a plan for the use of broadband infrastructure and services in advancing public safety and homeland security." We seek comment on how to interpret and implement this directive, including an analysis of existing policies and programs that are on point. We seek comment on how to identify which broadband services are most needed to advance public safety and homeland security. For example, should the Commission focus on broadband high-speed Internet connectivity for public safety and homeland security needs? How should the broadband infrastructure be designed in order to support both the needs of the public for connectivity to the global Internet and the needs of emergency services for connectivity to a restricted, private IP infrastructure? We seek comment on how advancing public safety and homeland security is interrelated with improvements in telehealth and telemedicine delivery through broadband. We also seek comment on how access to broadband capability may promote interoperable wireless-based communications among various public safety agencies and jurisdictions, as well as plans and benchmarks to improve interoperability. Similarly, we seek comment on how access to broadband capability in general and specific broadband services in particular will ensure that broadband-based applications and support systems (over any broadband transport platform) are compatible among different public safety agencies.***
	• It is currently not cost effective to build two separate networks – one for public and one for Emergency Services/Public Safety – but there will have to be features built in that will not only carry forward the current VPN capabilities of today's network, but additional enhancements to ensure that Emergency Services/Public Safety data packets are totally secure and safe from accidental or deliberate interception from unauthorized users • Agencies are currently able to tie different radio systems together using devices such as the ICU2000, but they are limited by geography • A widely available broadband connection among geographically dispersed agencies would allow such systems to function over

	a much wider geographic area • As advances are made in handheld units, it should be possible to build such a capability into the handheld unit itself • That is a future development that will be spurred once the availability to the broadband public safety network is there • The adoption of broadband connectivity and cost of service to Public Safety should be kept low enough so that agencies can afford to implement technologies that are based on broadband connectivity. • Mobile VPNs – Net Motion, Columbitech, Motorola Airbeam Safe – have FIPS 140-2 security that include persistent sessions, transaction resume, static/dynamic addressing and predetermined routing of users to different network services • These products allow Public Safety users to use whatever network is available and to switch seamlessly between different networks based on rules developed at the software level. • Use of VPNs allows Public Safety traffic to be carried on public networks, thus reducing operating costs for both groups of users • The National Broadband Plan should include elements that require public networks to pass VPNs (it's currently not universal) • Agencies can rout connections from VPN servers to private IP infrastructure and the internet • VPN-based connections with appropriate authentication and permissions can be established between different agencies for interoperability • Web-based applications provide access for all users with appropriate credentials
73	***We seek comment on whether and to what extent the national broadband plan should address means to protect and advance cybersecurity, specifically with respect to those broadband networks critical to the nation's critical infrastructure, financial institutions, public safety and homeland security. If so, what steps should be taken to secure the nation's most vulnerable broadband facilities and data transfers from cyber threats, such as espionage, disruption, and denial of service attacks? Should certain broadband service providers and operators adhere to specific standards or best practices to minimize such threats? Should the Commission adopt a process whereby communications providers can certify their compliance with specific standards and best practices? What agency or organization within the government is best positioned to take the lead inter-agency coordination role for protecting against and responding to cyber security attacks?***
	• Broadband services are easy to set-up and use in urban and highly populated areas • Rural areas are most disadvantaged – not easily installed or currently available • Public Safety wants access to NCIC returns for officers in the field; "near" real-time video for Fire and SWAT • Rural Public Safety agencies would also love to have these capabilities • Network needs to be private to protect information from outside sources
74	***We seek comment on any special concerns about ensuring physical diversity or redundancy in public safety and critical infrastructure industry networks and how to track and measure these factors. We seek comment on these issues with respect to commercial networks, as used by public safety entities for emergency communications. We also seek comment on strategies for improving network redundancy and hardening network assets.***
	• See bullets for Sections 72-73, above.

75	***We seek comment on how developments in broadband technologies and broadband-enabled services impact public safety and homeland security goals. Specifically, in preparing a national broadband plan, how should the Commission take into account the advent of advanced commercial wireless broadband technologies, such as LTE and WiMAX? Are "off-the-shelf" solutions sufficient? Why or why not? What broadband policies would best promote the deployment of next generation 911 (NG 911) networks, including emergency services IP networks? How might the results of NTIA's obligation under the NET 911 Act to develop an NG 911 migration plan assist with ensuring access to broadband service by public safety answering points (PSAPs) and establishing appropriate benchmarks?***
	• WiMAX has not been developed for mobile use and has a limited range in these applications • LTE could be a replacement for current 3G networks and may be the option for Public Safety depending on coverage areas • Off the shelf can work in urban but may not be available in rural communities • Should the FCC need to have LTE pushed into more rural areas for public safety, when vendors may balk at the costs and lack of ROI • NG911 systems may/will need to push information that is received via email or other IP-based technologies to the responding units • This may require an interface between NG911 systems and IP-based network that is being used for mobile data • Off the shelf systems, traditionally, have not had the reliability or level of security needed for public safety applications • The formation of a standardized NG911 ANI/ALI display format for all 911 centers across the US would help • As we move to NG911 that incorporates IP-enabled devices, the necessity for any 911 Center to transfer a call, and its associated data, to other centers across the country will only increase • NENA has already started working on developing a standard and it would be good to support what they have done and to take part it that development. • Public Safety should leverage advances that are occurring in broadband technology that are being developed to serve the public and commercial interests • Cost must be kept low or agencies will not be able to adopt data networks • Low-cost, off-the-shelf, components are a key element of cost reduction • NG911 assumes that both citizen and PSAP have internet connectivity • To make NG911 function, both ends of communication need to be addressed • PSAPs that don't have broadband connectivity should be supported in obtaining it • Publicly-supported secure wireless networks could be required to include a feature that would allow any user the ability to access the local PSAP whether they were a customer of that network or not

76	***We seek comment on how the public safety, homeland security, and health care communities envision using broadband both near-term and in the future. Specifically, what features are most important: live video; data transfer; web access; IP-based voice; security and encryption; mission critical or emergency use; virtual private networks; deployable systems for special events, disasters, and pandemics? What are the costs to public safety entities of obtaining broadband service (whether commercial or self-provisioned), devices, and applications, and what sources of funding are available? Are there opportunities for pooling resources, such as shared infrastructure? What models, such as statewide networks, have been tried and shown successes or limitations? What broadband networks exist or are planned? How are public safety entities currently utilizing or planning to utilize commercial broadband networks to carry out their missions? Are such networks used for "mission critical" communications? Are there accommodations that commercial carriers have made for public safety users, such as increased geographic coverage, back-up power, or hardening of facilities against weather or terrorist events, enhanced security, or enterprise customer discounts? At what cost? What limitations are public safety entities encountering with respect to commercial broadband networks, and what needs are going unmet by commercial offerings? We seek comment on how to achieve economies of network resource sharing by public safety, where there is "a dedicated broadband network that connects health care providers in a state or region."***

	• Security, data, VPN, deployable systems are a must
	• Information sharing – RMS, video surveillance
	• Secure voice and data communications
	• Funding is always a major issue
	• Cost to roll out a private system and maintain it are out of reach for many agencies
	• Commercial systems provide a reasonable cost, and they maintain the system
	• Politics can held and hinder a shared state system
	• Departments are upgrading their equipment to allow for increased and more efficient exchange of information (i.e., text, audio, video, etc.) to officers in the field – increases operational efficiency; no longer will field officers have to return to the station to get up-to-date information
	• This shift transfers a "mission critical" capability from an in-house system to a commercial vendor
	• Broadband connection will cost roughly $40-49 per month per officer
	• Additional hardware costs are minimal – air card cost will be absorbed by the vendor in the cost of the ongoing monthly connection fee
	• Increased transfer speeds also allows for access to the city's intranet, and local, State and Federal databases.
	• Public safety and critical infrastructure need prioritization
	• There should be broad support in the development of a National Broadband Plan for Public Utility Districts (PUDs) (non-profit) that are subsidizing the deployment of broadband connectivity
	  • In Washington State there are several electrical PUDs that provide fiber-optic network connectivity for control of their electrical distribution systems as well as expanded use for the public
	  • These networks provide a high bandwidth backbone at some locations and, at others, they provide fiber to individual residents and businesses

	• Under Washington State law the PUDs can only wholesale the connectivity, so third parties act as retailers for direct or wireless connectivity to the fiber systems • Public Safety has taken advantage of the PUD fiber-optic network to connect remote offices and to support WAPs • VLANs on the network or any network can allow different users traffic to remain separated • VPNs then provide an additional level of security • Grant County is also testing low cost 802.11 access points and radios on 900 MHz, 2.4 GHz, 4.9 GHz and 5 GHz. • These radios, combined with the PUD fiber-optic backbone will supplement the commercial cellular data in areas of limited or no coverage
77	***The Commission has previously found that wireless broadband services will play an essential role in the ability of public safety entities, especially first responders, to fulfill their mission to protect the health, welfare and property of the public. What role should existing fixed and mobile spectrum allocations, which are able to support public safety broadband deployments, have in the development of a national broadband plan? Specifically, how can the 4.9 GHz band meet the broadband needs of the public safety community? In developing the national broadband plan, what is the interplay with our current rulemaking addressing public safety services in the 700 MHz band? For example, in a separate proceeding, the Commission is seeking comment on how to promote the development of a nationwide, interoperable broadband network for the nation's first responders. What additional steps should the Commission take with regard to other spectrum bands available for public safety use, such as the 4.9 GHz band, in order to help meet the broadband needs of the public safety community? What special considerations, concerns or limitations should be taken into account specifically with respect to public safety broadband deployments in rural areas?***

	• The potential exists for low cost data solutions if the appropriate clean spectrum is made available. For example:
	  • Grant County Sheriff's Office and Technology Services (Washington State) has been doing testing with 802.11 based radios for about 2 ½ years
	  • Using Ubiquiti 400 mw 4.9 GHz radios ($260.00) with 14 db 120 degree sector antennas delivering to 6 db mobile antennas Grant County Sheriff's Office and Technology Services learned that tree foliage stopped the signal and that usable range was very limited
	  • This seems to be consistent with the intense number of access points that are deployed with successful 4.9 GHz deployments
	  • Intense access point deployment with its associated cost limits the potential for 4.9 GHz delivery to mobile units
	  • 4.9 GHz is very viable with higher gain flat panel antennas for video links from fixed locations or for backhaul between access points, but it does not deliver well to mobile omni antennas
	  • Radios with full legal power may also make 4.9 GHz more attractive in the future than it is today
	  • In comparison, testing with Ubiquiti 700 mw 900 MHz radios ($130.00) provided 1 Mb per second through trees and residential structures for about a 1 ½ mile radius. Line of sight coverage at 1 Mb per second was available to about 2 ½ miles with through put dropping off beyond that to about 2.8 miles. *(readings were obtained in an environment with a -87 to -88 noise floor on a 10 MHz channel)*
	  • Ubiquiti has a similar 700 MHz radio available for $280.00. All of these radios require a network board, software and cases but can realistically be assembled with two radios and antennas for less than $1,000 per car or access point.

- The availability of low cost equipment that local agencies could deploy would become a viable option if the two 10 MHz segments of the D-Block spectrum is returned to local deployment for public safety
- 4.9 GHz couples nicely with this approach for backhaul to other networks including licensed microwave that public safety agencies may already have in place
- An additional consideration for this approach is public safety traffic on the TV white space UHF channels. Some licensing mechanism would need to be present that would assure that an investment in equipment in this band would not be wasted by a new TV station coming on the air. The TV white space spectrum is particularly of interest in rural areas as they will have fewer TV stations and more available spectrum
- LTE is a technology of interest, if it can be moved to the needed frequencies and the price points make it viable for agencies to deploy

- Brookline, Massachusetts has entered into a Public/Private Partnership with an ISP to provide a border-to-border Wi-Fi network, using 2.4 GHz (for municipal and consumer use) and 4.9 GHz (for public safety use). Here are some highlights:

  - Wi-Fi communications in the past operated and relied on purchasing vendor specific wireless systems. In Brookline's case, its PD has 40 air cards costing $50.00/month each, which is limited in capacity, has many dead spots, low bandwidth, and is prone to interference from other sources. Now, through its ISP, Brookline is operating on a 4.9 broadband Wi-Fi network that covers the entire community (6.8 square miles) and will save the PD $2,000.00 a month, equal to the cost of the Verizon CDMA air cards. When using the air cards, Brookline had limited access to its internal databases due to network configurations and the limited bandwidth that the air cards use.
  - Brookline has terrible cell coverage, regardless of the carrier; with the 4.9 network, Brookline has plugged all known dead spots.
  - If more bandwidth is required for an incident, the PD has the ability to take over the entire 2.4 network to aid it during an emergency.
  - The 4.9 network, along with NetMotion software, allows Brookline's officers to access all public safety databases from their vehicle mounted laptops. The 4.9 wireless network is connected into the internal public safety network; because of this configuration, Brookline PD is able to use our active directory service, anti-virus software from its AV server, and WebSense filtering, users get the same rights and restrictions as if they were logged into the internal network, along with the network security and firewall rules that are incorporated in the public safety network. For all management purposes the 4.9 network is an extension of Brookline's internal public safety network.

    Brookline is running the following applications over the 4.9 wireless network:
    - Public Safety applications from Larimore Associates - some of these are CAD, RMS, Arrest, FI, Training, and Scheduling to name a few. When using the air cards Brookline PD only had access to the RMS using a thin client application. The coverage issues caused this application to crash on a frequent basis. It was so bad officers would not even try to write a report from the vehicle, they would return to the station and write the report from headquarters. Now, with the 4.9 wireless network, officers are entering all the standard reports from their vehicles, which keeps these units

	in their own patrol sector, and can respond to calls while writing these reports without fear of losing their work. Brookline PD has the ability to handle silent dispatching, (CAD system to vehicle), Arrest database for arrest mug shot information, inputting Field Interviews directly from the field, and many other applications that where developed through its Public Safety software suite. • Access to the traditional State databases for stolen vehicles, registration information, wanted persons, etc. • The Wi-Fi system allows officers to access a closed, internal email system from their vehicles, Brookline PD has also given its officers the ability to access all General Orders, Policies , Directives, Special Orders, Crime Bulletins, COM Stat reports, Crime Stats and Mapping information, training materials, (Brookline PD is working on sending out a training video to the field at this time, as well), Emergency Management databases, that have all the schematics and general information for our schools, both public and private, including local colleges. • The Wi-Fi network allows Brookline PD to bring GIS applications into its vehicles; this is a high bandwidth application (ArcGis) which could not run over the CDMA Verizon network. • Officers can also access camera feeds to their laptops. Brookline has two (2) camera networks, one is a Critical Infrastructure Camera Monitoring System, and the second system has cameras deployed in crime areas, using the 4.9 mesh network. These wireless cameras can be placed anywhere within the Town borders and are configured to run on the Wi-Fi network. • Voice over IP (VoIP) – working on a pilot project to test this technology out in the near future. • Radio over IP (RoIP) – working on a pilot project to test this technology out in the near future. • Brookline PD has found no interference issues on the 4.9 network; however, it has found the 4.9 signal will propagate longer distances than the 2.4 signals, due to all the interference in the 2.4 spectrum. • The system is using all Strix hardware, the access points, vehicle mobile units, backhaul etc. Brookline built the network once to accommodate the public and public safety. The hardware can accommodate 6 different radios. Brookline has three (3) spare radio slots available to add WiMAX or 700 MHz, so expanding the system is just a matter of placing new radio cards in the nodes, the network can grow with the future. In the event of an emergency, public safety can take all the bandwidth from the 2.4 network side, if needed. • Brookline can set up a fully functional, on-scene command post with a few laptops, accessing all the above mentioned applications. • The 4.9 Wi-Fi network is also tied into Brookline's EOC, which has an access point installed within the EOC for accessing the 4.9 and 2.4 networks. • **Problem Issues**: • The user only has coverage within the borders of the Town, to solve this we will keep 6 to 8 air cards active that will be configured with NetMotion to switch over to the Verizon CDMA network when the 4.9 signal is lost. • No vendor is offering a hardware solution for hand held units that have 4.9 built-in • Brookline's solution has been to configure a secure VPN tunnel over the 2.4 wireless network for these units, again using NetMotion to manage the connection.
78	***In the instant proceeding, we seek comment on what part, if any, the development of an interoperable public safety***

	broadband network should play in the overall plan for the use of broadband infrastructure and services in advancing public safety and homeland security. We seek comment on whether there are programs at other agencies that should be considered as a part of the national broadband plan. We also seek comment on what lessons the Commission can incorporate from its existing policy roles impacting public safety and homeland security. Finally, we seek comment on how plans and efforts to advance public safety and homeland security should be coordinated between and among the various federal, tribal, state, and local entities.
	• One of the greatest needs in a true emergency is to be able to deliver information to the public in a quick, targeted fashion • Currently, there are several vendors who offer mass notification systems (Reverse 911) • A need exists for a system that can handle large-scale, geographically targeted notifications with ease • This might involve developing new capabilities into future cell phones that could receive messages over that frequency independent of vendor and not dependent upon individual line capacity of the local landline phone infrastructure, or new communication/computer devices in the future that are able to receive public safety announcements from the same system, or both • A high speed, high capacity, geographically targetable message delivery system from public safety to the general public
115	***We recognize that public/private partnerships have historically achieved public goals in innovative ways. We seek comment on ways in which public/private partnerships can collaborate to advance common broadband objectives. Likewise, we seek comment on cooperatives, including their successes and potential to meet the broadband needs of communities around the country. We ask how public/private partnerships should be structured to ensure that objectives are reached in a timely and efficient manner. Would such partnerships be more effective on a Federal, State, local or Tribal level? We also seek comment on any past successful broadband public/private partnerships, as well as specific proposals for public/private partnerships in line with the objectives of a national broadband plan.***
	• A high speed, high capacity, geographically targetable message delivery system from public safety agencies to the general public