# The FCC Plan for a Public Safety Broadband Wireless Network

Jennifer A. Manner, Stagg Newman, Jon M. Peha

## Abstract

In March 2010, the U.S. Federal Communications Commission (FCC) released the National Broadband Plan (NBP) for the United States, which made significant recommendations for improving access to broadband communications across America including for enhancing the role of broadband for public safety and emergency response. In particular, the NBP proposed a novel, data-driven and comprehensive strategy for creating a nationwide interoperable public safety broadband wireless network for first responders and other public safety personnel. This paper presents details of this strategy, focusing on those novel elements that represent a substantial departure from the approaches of the past, including the following. Rather than relying on many independent systems, a consistent and coherent network of networks would be deployed throughout the nation, and new governance structures and technical regimes would be established to maintain interoperability over time while reflecting public safety needs. To reduce costs and expand capabilities, the system would leverage widely available consumer electronic commercial technologies and commercial infrastructure in innovative ways, including a form of incentive-based partnership that allows infrastructure-sharing without compromising on public safety's stringent quality requirements. Rather than relying on a single system to meet all communications needed, this multi-faceted strategy would provide greater capacity, resilience, coverage, and versatility by giving first responders access to a broadband network built out for public safety, commercial cellular networks, satellite services, in-building devices, and in-vehicle devices that can be deployed where needed.

## 1 Introduction

The safety of every citizen is highly dependent on the ability of first responders to communicate effectively in an emergency. While the capabilities of both commercial and military communications systems have vastly improved in recent years, the same cannot be said for the systems used by most public safety agencies in the United States. These systems generally provide traditional voice communications, but lack support for broadband, geolocation, and other valuable features that are commonplace on commercial networks. As the 9/11 Commission [1] and others have concluded, today's public safety communications systems are prone to interoperability problems, which make it difficult for first responders from different agencies and geographies to communicate and coordinate. And as observed after Hurricane Katrina some systems may need greater dependability and resilience to provide basic operability after a serious disaster [2]. Moreover, when compared to a communications system built from modern technology, the public safety systems in the United States are quite expensive, and are very spectrally inefficient [3, 4]. Thus, there is great need for a nationwide interoperable and highly dependable broadband wireless network built from cutting-edge technology, but to achieve this, a new policy approach must be adopted.

In March 2010, the U.S. Federal Communications Commission (FCC) released the National Broadband Plan (NBP) for the United States [5], which made significant recommendations for improving access to interoperable broadband communications across America and for enhancing the role of broadband in public safety and emergency response. In particular, the NBP proposed a novel and comprehensive strategy for creating a public safety broadband infrastructure, and recommended that $12 to $16 billion be allocated in public funds over ten years to implement that strategy to pay for capital and on-going expenses.

The NBP strategy differs from past policies in a number of crucial respects. Public safety communications has generally been considered a matter for state and local public safety agencies, leading to the deployment of many thousands of separate and often incompatible networks**.** In many cases, separate networks serve different agencies in the same town. In contrast, the NBP strategy assumes a single nationwide architecture utilizing a network of networks approach. All first responders in a single location can use the same network. It is far simpler to maintain a coherent nationwide technical approach and infrastructure that is shared across local many local agencies when funding comes from the federal government, so there is reason to establish a new and cost-effective funding mechanisms within the federal government designed specifically to cover the initial costs of deployment and the ongoing costs of maintenance and operation. It also requires new institutions at the federal level to ensure interoperability, as well as new types of advisory committees to ensure that the perspectives and expert knowledge of local public safety agencies reaches their federal counterparts.

The NBP strategy also reflects an entirely new view of commercial technology and commercial infrastructure. Public safety communications systems emerged long before the invention of cellular telephone systems, so it is perhaps no surprise that there is little sharing of infrastructure between commercial networks and public safety networks, and that much of the technology used in public safety networks was developed exclusively for the public safety market. However, times have changed, and the large and competitive market for cellular equipment has yielded better and more reliable devices at reduced costs, while commercial infrastructure has become increasingly pervasive and dependable. The NBP seeks to take full advantage of these developments, while simultaneously ensuring that public safety's stringent requirements are met. As this paper will show, this includes making use of emerging commercial technical standards, sharing towers and back-up power, backhaul and core network IP infrastructure with commercial providers, and using capacity on commercial networks during the more serious emergencies on a priority basis.

Section 2 will describe the past and present policies for public safety communications in the United States, and Section 3 discusses in greater detail the need for evolution, including greater reliance on commercial technology. The uniquely multi-faceted nature of the NBP strategy is presented in Section 4, followed by more detailed discussions of critical aspects of the plan. Section 5 presents ways to meet public safety's capacity and quality of service needs, while Section 6 addresses innovative ways of reducing costs. The institutions designed to provide nationwide interoperability are discussed in Section 7. Finally, the paper is concluded in Section 8.

## 2 Lessons from Past U.S. Policy on Public Safety Communications

As discussed in Section 1, the nation's approximately fifty thousand public safety agencies have produced a highly fragmented infrastructure consisting of many thousands of independent systems under different administrative control, using a variety of technologies. This has tremendous disadvantages when compared to a single cohesive network designed to serve the entire nation [3]. Consider the implications for dependability. The most widely discussed problem with public safety systems is that lack of interoperability can undermine communications whenever multiple agencies or agencies in different geographies attempt to cooperate. The use of multiple potentially incompatible technologies leads to interoperability problems. Dependability is also reduced because first responders are limited to a single system. For example, a firefighter on the Gulf Coast may be in easy communications range of the transmission towers of four different public safety agencies, but his mobile device is only set up to communicate with his own fire department's system. If that system happens to fail during a hurricane while the other three are left standing, he loses the ability to communicate unnecessarily.

This traditional approach to public safety communications has also made the systems extremely costly, in a variety of ways. First, the cost of building and operating infrastructure is roughly proportional to the number of antenna sites needed, and public safety agencies have deployed more than an order of magnitude more antenna sites than would be needed by a single nationwide cellular network with comparable functionality and coverage [4]. Second, although it is not always explicit, another major cost of wireless systems is their allocation of valuable spectrum. It has been shown that U.S. public safety communications systems consume an order of magnitude more spectrum than needed due to their low frequency reuse, which is the inevitable result of fragmentation into thousands of separate systems, combined with use of non-cellular technologies [3]. These spectrum inefficiencies would be even greater in a broadband system, because the minimum allocation for each system would be much larger. Third, the cost of public safety equipment is high. The high cost is driven by the small volumes, extreme market fragmentation of public safety market, and the limited number of suppliers, as will be discussed further in Section 3.

Because of these factors, it should be possible to bring broadband data services to public safety, to overcome many of the interoperability and dependability problems of the past, and to do so at vastly lower expense to tax payers by giving public safety access to a cohesive nationwide broadband network that leverages the commercial technology and infrastructure while still meeting the unique needs of the public safety community. The first U.S. Government policy intended to create such a network was developed by the FCC in 2007 [6]. The objective was to establish a public private partnership, whereby a commercial entity would deploy a system that serves both public safety and the general public. 10 MHz of spectrum nationwide would be assigned to a public safety representative, and another 10 MHz would be auctioned. The winner of this auction would be able to serve paying customers in the entire 20 MHz, but would be required to build their network in accordance with public safety requirements, and to serve public safety on a priority basis in 50% of this spectrum, or in the most severe of emergencies, 70% of this spectrum. The precise requirements and obligations would be determined through negotiation between the commercial and public safety licensees after the auction. Ultimately, the

spectrum was auctioned, and, no one was willing to make the minimum bid. At present, the spectrum remains unused, and no nationwide network is being deployed.

Many important lessons from this auction can help guide future policy. First, the comments of many wireless service providers and equipment vendors demonstrate that commercial companies could be interested in exploring novel relationships with public safety and new technical approaches to meet public safety needs. Moreover, interest within the public safety community in a nationwide broadband network for public safety use also grew considerably. However, the apparent interest on both sides did not lead to a successful public private partnership, due to a combination of reasons [7]. One important reason is that obligations and requirements were not fully specified before the auction leaving uncertainty. It has been shown [4] that seemingly modest changes in some of public safety's technical requirements, such as the maximum data rate per device or the signal reliability, can greatly affect the cost of deploying a network. Thus, any uncertainty about such parameters or about important financial terms could easily deter parties from bidding, even if an agreement could have been reached that would benefit all parties. It is therefore important to make decisions about such issues early in the process. There is also reason to reexamine the financial viability of the public private partnership envisioned in that particular auction. In the most densely populated regions, potential bidders can expect that the value of the spectrum they gain access to will exceed the cost of meeting public safety needs. However, it turns out that in most of the country, including the rural areas and many suburban areas, if the public private partnership must build a network that can meet public safety's strict requirements, this is probably not the case [8]. Thus, policymakers must either compromise on meeting public safety requirements, compromise on how much of the nation will be served by this "nationwide" network, or find some other means of covering network costs beyond granting access to this spectrum. Finally, we may learn lessons regarding geographical scope. The license in this auction was to be nationwide. This has many advantages, including decreasing the risk of interoperability failures where networks come together, but there is also a risk that smaller carriers will be discouraged from bidding. Consider a regional wireless service provider. In its own region, it may be able leverage existing infrastructure to serve public safety at lower cost, but it cannot do so in the rest of the country.

## 3. The Need for Evolution

One of the consequences of the current public safety model for communications is that it relies on out-dated proprietary [9]. Traditionally, because the market for public safety communications equipment is so small, prices are high because manufacturers cannot recover costs over wide customer bases. Instead, the small number of potential public safety consumers (estimated between 1 and 3 million) means that costs for equipment development and manufacture must be spread across a very small customer base. This means that public safety is burdened with significantly higher equipment and device costs than those available in the consumer electronics marketplace. For example, a police department may spend $3000 to 5000 per voice and low speed data (narrowband) P25 handset carried by its officers. In contrast, a handset built to TETRA standards with comparable features costs under $1000. TETRA is the global standard for narrowband public safety devices used in many countries outside the U.S., Production volume for TETRA is much larger, in part because in many countries, the market is driven by

nationwide systems with large numbers of users rather than many small localized public safety systems. Total systems costs for TETRA are also typically several times lower than for comparable P25 systems. [10]. As another example, ruggedized cellular phones such as the Motorola Brute i680 meet military specifications for dust, shock, vibration, and temperatures, are produced in larger volumes so they can be sold for a few hundred dollars each [11].

Because of the high cost of equipment, coupled with difficulties that the public safety community has in receiving funding for new equipment as they are reliant on non-predictable public funding, public safety will often have to rely on decades old communications technologies and network equipment. Accordingly, unlike consumer markets where devices are switched out on average every couple of years, public safety may utilize the same devices for a decade or two. This means that they are not able to benefit from technological innovations. Similarly, because of this low turn around time and the lack of a large consumer base, equipment vendors that serve the public safety community have fewer market incentives to innovate in this sector. Further, some equipment vendors market proprietary technologies as a means to keep market shares high. This means that innovation in this sector may be slow to emerge.

The key to cost effective technology is creating a large volume market that enables common costs such as research and development and other non-recurring engineering costs and factory production lines to be shared over many millions of units of equipment. As the market grows in volume over time, the costs of handsets decline to a small fraction of the introductory cost as has been seen repeatedly in the cellular industry [12, 13].

The deployment of a public safety broadband network that leverages consumer technologies and network design can change this paradigm dramatically. For the first time, if public safety deploys using a widely-deployed consumer electronic technology as the underlying basis, public safety can benefit from the cost and innovation benefits of such technologies even if the end devices are subsequently specialized to meet public safety needs. In particular, a number of public safety groups, including the National Public Safety Telecommunications Council (NPSTC), the Association of Public Safety Communications Officers (APCO), and the National Emergency Numbering Association (NENA) have all agreed that the broadband wireless public safety infrastructure should be built using the Long Term Evolution (LTE) standard, the global standard for 4G selected by most major carriers [14, 15, 16]. By leveraging consumer electronic LTE devices, public safety should be able to receive devices and equipment at lower costs then they do now. This is because competition in the marketplace and the ability to serve broader consumer groups result in lower prices, particularly for chip sets and other common components that go into a handset.

This does not mean that commercial and public safety end-user devices will be identical. As long as the high cost components are shared, end-user equipment can be customized for unique user needs without great expense. For example first responders will need "ruggedized equipment," but that equipment can share many of the components with large commercial markets. Figure 1 below shows key components of end-ser devices, the degree of commonality between commercial and public safety devices, and the effect of customization of cost. We see that the components that are most costly to customize are also those that can most easily be common to both commercial and public safety devices. Thus, with common standards, operating

systems, and chipsets, public safety's ruggedized devices can be provided at relatively low cost. This is especially true if public safety partners with commercial service providers in the same frequency band.

| Component ==> | Hardware | Software/ Middleware | Operating System | Baseband Chipset | RF Chipset | RF Front End |
|---|---|---|---|---|---|---|
| Degree of commonality to commercial devices | Medium | Medium | 100% | 100% | 100% | Low |
| Effect of customization on cost | Low | Medium | High | High | High | Low |

Cost of customizing the highest cost components will NOT be incurred because they are 100% leveraged

Figure 1

Further, because public safety will be able to leverage equipment that is available in the consumer electronic market, public safety will be able to benefit from innovation in the commercial market-place and network evolution on a cost-effective and timely basis. In fact, many of the features that were originally principally used by public safety in the past, such as talk groups, high security networks, and command and control priorities, are planned for releases of LTE, the global standard for 4G cellular networks [17, 18]. Moreover LTE networks will be increasingly used by enterprises to support mission-critical enterprise applications. In the same way that there has been increasing synergy between demanding wireline enterprise and critical government network requirements, there will be increasing synergy between enterprise wireless LTE networks and public safety networks. Thus, a plan is needed that can exploit these synergies and meet public safety's unique needs.

## 4. Multi-faceted solution for public safety communications

First responders must communicate in a wide variety of circumstances, from deep inside an urban skyscraper to a remote rural location. They may be communicating while stationary with a handheld device or from a vehicle moving at very high speeds. The challenge of providing a cost effective broadband infrastructure for public safety is further complicated by the fact that an incident may require a high concentration of first responders in a focused area. Policy and technology must be designed to meet these diverse needs.

Different approaches have different advantages for first responders. For example, some have considered the relative merits of a terrestrial wireless network dedicated to public safety, such as the Integrated Wireless Network [19], and a terrestrial wireless network that serves both public safety and paying customers, such as the FCC's public private partnership [6, 20] discussed in Section 2. Cost studies have shown that there are tremendous efficiencies associated with sharing both spectrum and infrastructure [4]. However, a public safety network requires a high degree of coverage and signal reliability when compared to commercial networks. In other words, a first responder must be able to transmit with high probability, even in locations that are of little interest to commercial providers. Public safety networks also require a greater degree of

hardening. Better coverage and greater hardening increase costs. When a network is shared, and its revenues come primarily from commercial users, one must find effective methods to ensure that the network is nevertheless built out to public safety rather than commercial standards, and this network continues to meet public safety standards year after year even as both technology and public safety needs evolve over time [21]. Rather than choose between these alternatives, the multifaceted NBP approach would use both of these, and more. A nationwide network would be designed and built out in spectrum allocated specifically to public safety to meet public safety's strict standards for coverage, signal reliability, and hardening, now and in the future. At the same time, roaming onto commercial wireless networks would bring the many benefits of sharing. Such roaming provides additional communications capabilities that could be used either when the primary network is congested due to high demand and more capacity is needed. or when the primary public safety network fails at a particular site due to a natural disaster or deliberate sabotage or other cause, or. As was seen in Hurricanes Gustav and Ivan, the commercial networks may be operational in areas where public safety networks have failed

Therefore the NBP plan recommends the multi-faceted broadband infrastructure shown in figure 2 below (taken from [5]). This will provide public safety with much better coverage, reliability, capacity, and cost effectiveness than any single network approach could provide.

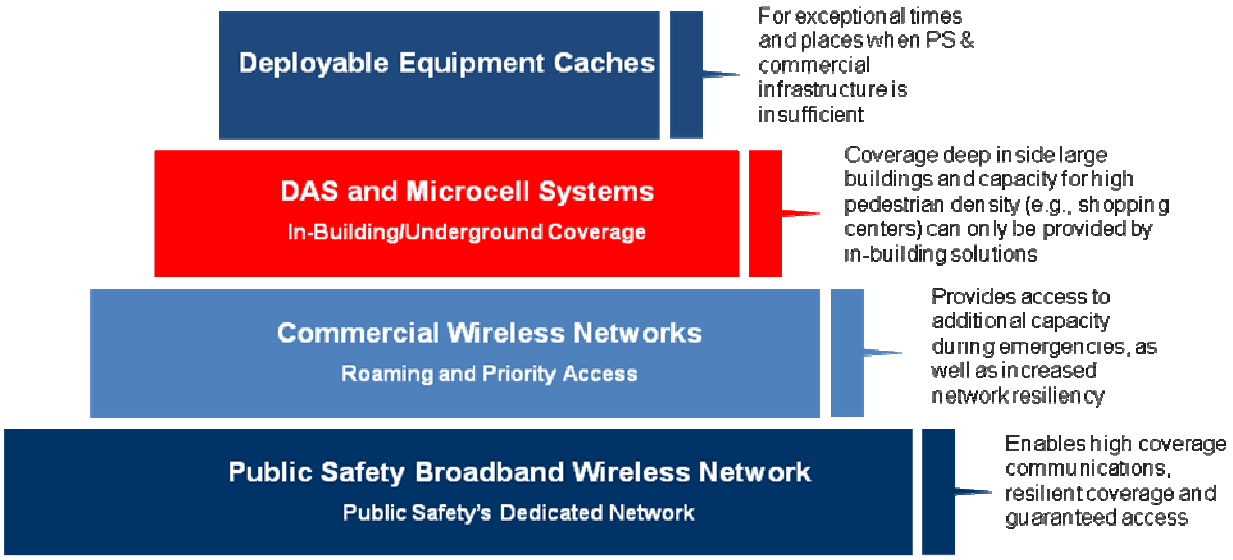



Figure 2

First, at the base of the pyramid, the core of the infrastructure is a nationwide cellular infrastructure using 4G LTE cellular Radio Access Network technology within dedicated 700 MHz paired broadband spectrum for public safety. As discussed further in Section 6, this network would leverage commercial assets such as cell sites and backhaul that would be "hardened" to public safety standards. The network will initially provide broadband data and video and commercial voice services, as provided in LTE 3GPP releases 8 and 9. As LTE matures, equipment will be deployed that is capable of fully supporting all mission critical services, such as the command and control voice talkgroups supported today by public safety LMR networks.

Second this core network is complemented by priority access on commercial networks that provide additional capacity and provide coverage when the public safety network is unavailable. The capability to provide this type of priority roaming is built into LTE 3GPP Release 10 and is already well established both in wireline IP networks as well as in IP networks for the military [17, 18, 22, 23, 24].

Nevertheless no cellular network, neither commercial nor public safety can cost effectively provide the coverage needed deep inside larger buildings, particularly at the high speed transmission rates required for advanced data and incident video services. So third, high quality wide area systems would be complemented by in-building solutions, especially for larger buildings. The cost of providing in-building coverage is dropping dramatically with the continuing development of pico-cell, femto-cell, and distributed antenna system technologies. Moreover, more and more commercial buildings are being installed with in-building systems that "light-up" commercial cellular spectrum. This provides the opportunity to either use a priority wireless service in the commercial spectrum and/or light up the public safety spectrum leveraging the commercial assets. Furthermore LTE Release 9 and 10 will have enhanced features such as enhanced Home Node B, Self Organizing Networks, and Relays that will enable interoperable communication with effective in-building systems as noted in the LTE Standards Evolution Chart above. Even in residential and smaller business buildings, the problems of in-door coverage are being mitigated by the deployment of femtocells, which typically connect directly to the wired infrastructure. It is already in the interests of commercial carriers to deploy femtocells because they provide capacity relief for the explosion of data traffic, and do not consume wide area spectrum resources. Thus, the availability of priority roaming onto commercial networks together with a femtocell supporting that commercial service can enable first responders to communicate in places within buildings where they could not otherwise do so.

Fourth, first responders would have two types of deployable equipment to provide or supplement coverage or capacity for i) remote or hard to cover areas; ii) emergency communications when the normally available infrastructure has failed; or iii) focused capacity is needed at an incident location. The first type of deployable equipment would be caches of mobile deployable cell sites. These systems, referred to today as COWS (Cell on WheelS) and COLTS (Cell on Light TruckS), are already available today for cellular operators. LTE enables a new generation of this equipment that will be much lighter than current equipment. In fact, China has taken the lead in making new rapidly deployed equipment available for emergency responses and has used such equipment to respond to recent earthquakes [22, 23, 24].

The second form of deployable equipment would be placed in first responder vehicles, effectively turning those vehicles into pico-cells or repeaters. For example, when a police officer leaves the vehicle to go into a building or to the physical site of an accident (*e.g.*, to investigate a car rolled over an embankment or to pursue a suspect on foot), the officer's hand-held device can communicate back to the communications system in the vehicle, which then communicates back to the closest cellular tower—perhaps using a high-gain vehicular antenna. By using such an approach, the quality and speed of communications will be much improved, so that high speed data and incident video can be supported even in low density areas.

Ultimately satellite systems should complement the terrestrial broadband infrastructure, for two reasons: i) there will always be some remote locations such as wilderness areas where there will be no terrestrial solutions, and ii) in the event of horrific natural or man-made disasters that destroy terrestrial systems, satellite provides a back-up capability of last resort [25]. Recommendation 16.3 of the National Broadband Plan ([5], p. 320) calls for satellite as part of the overall solution. Further discussion of satellite systems in beyond the scope of this paper.

## 5. Meeting Capacity and Quality of Service Needs

As described in Section 4, under the NBP, public safety's baseline communications capabilities will come from a network designed specifically to meet public safety needs. In this section, we focus on two particular types of needs: signal reliability and quality of service at the edge of cell, and aggregate capacity.

Needs must be met throughout the country, although not necessarily in precisely the same way. Rural areas offer particular challenges. As shown in [4], the marginal cost per person covered in the United Statea begins to increase significantly when the population covered by a network reaches 95%, and this cost increases much more rapidly when the population covered exceeds 99%. When covering this 95% of the population, one is serving all urban and suburban areas in the United States, and many rural areas as well. We observe that in the remaining portion of the country, which consists of sparsely populated rural areas, motor vehicles will play an important role in emergency response. Thus, as described below, we can adopt a somewhat different model in these sparsely populated rural areas.

Although it is not the responsibility of the FCC to design the next public safety network, it was the FCC's responsibility to estimate the cost of this network. This required a detailed understanding of the cost per cell site, which is addressed in Section 6, and the number of cell sites needed, which is addressed in this section. Baseline analysis was accomplished with a detailed analytic model, and fine-tuned through extensive coordination with experts in the field. The analytic model estimates the cell size needed to meet technical requirements in any given region, taking into consideration that region's geographic and demographic characteristics, e.g., dense urban areas are treated differently from hilly rural areas. For the basic methodology, see [4], but the FCC made different assumptions with respect to numerical inputs than in previous work.

One requirement that drives the number of cell sites needed is that the most demanding kind of device must be able to operate anywhere in a cell. This means the signal-to-noise ratio must be high enough that the probability exceeds a given threshold of a signal being properly decoded when it is coming from a mobile device transmitting at the maximum supported data rate and the maximum allowed power at the very edge of a cell [4]. Note that this criterion incorporates most of the usual quality metrics *except* capacity; it must be met even if there is only a single device. We initially estimated the number of cells needed using this criterion alone. Some of the important and atypical assumptions follow. We assumed that signal reliability, which is the probability that a user gets a sufficiently strong signal to communicate, must meet public safety's strict standards as defined by NPSTC [26]. Within the portion of the coverage area that covers

95% of population, i.e. all urban and suburban areas and many rural ones, we assume that signal reliability must meet this requirement indoors, and we use NSPTC's requirements for indoor penetration margins [26], which are particularly strict in urban areas where buildings can have thick cement walls. In the most sparsely populated areas containing 5% of the U.S. population, we instead assume penetration margins that are more appropriate for vehicles than for buildings, so indoor coverage can be less reliable in any buildings that are located at the edge of a cell. However, to further extend reach, we also budgeted for routers that can be placed in vehicles, and can relay IP packets from the wide-area public safety network to a local-area network that reaches first responders inside buildings, and vise versa. Finally, we assumed that the transmit power of mobile devices would be limited to levels that are appropriate for standard commercial LTE devices (e.g. 23 dBm), rather than the much higher power levels that have been used in the past for public safety handsets. This latter assumption further increases the number of cell sites needed. However, limiting ourselves to lower-power devices is consistent with our objective to let public safety use commercial off-the-shelf technology wherever possible, as described in Section 3. Thus, while this may increase the number of cells needed, it can yield much lower equipment costs, thereby saving money overall. Furthermore the deployment of high power subscriber devices in a broadband network can lead to substantive reduced capacity by generating more interference into the cell.

Using these assumptions, the FCC estimated that a public safety network should have roughly 44,800 sites [27]. This would make the public safety network the third largest in the United States, fairly close behind Verizon and AT&T, despite the fact that these commercial carriers serve on the order of 40 times as many users. Moreover, conservative assumptions such as those described above yielded an unusual result. In a typical commercial cellular network, a relatively small number of sites can be deployed merely to cover the desired area, but far more are needed to meet capacity constraints. In contrast, a public safety network using low-power commercial devices requires a large number of sites just to meet strict public safety signal reliability requirements, so a large capacity is difficult to avoid even with the relatively small number of public safety users expected. While the total number of sites is specific to the United States, this broader observation would be true in any nation that seeks to build a network to meet comparable public safety requirements. Thus, unlike commercial networks, much of the public safety network can be coverage limited.

This has a number of noteworthy implications. First, if not enough sites are deployed, this will adversely affect first responders' ability to get a reliable signal at edge of cell, rather than just the risk of congestion. Second, the number of sites and therefore total cost is far more sensitive to parameters that affect the performance of a single device at the edge of cell. In particular, increasing the data rate of mobile devices will greatly affect cost. According to the FCC model, increasing this data rate to 1.2 Mb/s would increase infrastructure cost by a factor of 2.85, largely independent of the amount of spectrum allocated [28]. One implication is that the hidden cost for high data-rates should be considered as one of the factors in the ongoing deliberation over what video data rates should be supported [29]. (There are technical means to reduce the impact of high-data-rate devices, e.g. by increasing transmit power and using more complex antennas, although use of less widely used technologies tends to increase device costs [28], as discussed in Section 3.) Regardless of how much spectrum is allocated, the only way to overcome this

impediment to supporting high-data-rate upstream connections for video or other applications on standard low-power devices is to deploy more cells.

In addition to the quality of service experienced by a single device at edge of cell, we must also consider whether the aggregate capacity needs of all devices will be met. As described in full detail in [28], one approach was to quantify aggregate capacity requirements in several specific emergency scenarios: a 2007 bridge collapse in Minneapolis that killed 13 people and injured 145, a 2008 category-4 hurricane that hit Houston Texas in 2008, and a hypothetical "dirty bomb" terrorist attack in mid-town Manhattan with 900 casualties. These may or may not prove to be the "worst case" scenarios, but by making specific assumptions corresponding to well-understood scenarios, we are able to assess whether the core public safety network would be sufficient in some demanding cases. For this particular analysis, we assume an LTE-based cellular system operating in 10 MHz of spectrum, with 3 sectors per cell, and perhaps most importantly, cell sizes consistent with deploying 44,800 cells nationwide to reach 99% of the population, which is consistent with the NBP.

The first two scenarios (Minneapolis bridge collapse and Houston hurricane) are based on data collected in actual emergencies by the FCC, but supplemented such that first responders would make use of a variety of communications capabilities that will become possible with a nationwide broadband network, such as video, file transfer, and emergency medical service (EMS) patient tracking. In both scenarios, we found that there was sufficient capacity to meet projected needs. Under a variety of assumptions, utilization never exceeded 75%. The third (New York dirty bomb) scenario uses assumptions proposed by New York City [30], in which multiple public safety agencies respond to the dirty bomb attack with a variety of mobile multimedia devices. However, we were forced to modify a few assumptions. The original proposal assumed that New York would be served by a mere 200 cells, which is not enough to support even 256 kb/s indoors, and it also assumed data rates for individual streams as high as 1.15 Mb/s. These assumptions are incompatible. If the number of sites is in accordance with NBP estimates, and video data rates are 256 kb/s, then utilization would be 58% in this scenario. With 512 kb/s video, it would be 79%. Quadrupling video data rates while keeping other applications unchanged would increase total traffic by a factor of 2.1, but if the infrastructure is designed so that this higher video data rate can be supported from a camera at edge of cell, then we need 2.85 times more cells, giving the system far more capacity to support the higher traffic level. This once again demonstrates how, in contrast to typical commercial cellular networks, edge-of-cell performance for a single device can drive network design and cost more than aggregate capacity requirements. It also shows that a network designed with enough sites to meet public safety's edge of cell requirements will have significant capacity.

Nevertheless, it is always possible to imagine scenarios that require more capacity. For such circumstances, the multifaceted NBP would allow first responders to roam onto commercial networks on a priority basis. Sharing of spectrum and infrastructure is particularly cost-effective for public safety because their need for communications capacity is modest most of the time, but with large spikes during emergencies [32], and it is these spikes we must accommodate. Without resource sharing, most of public safety's capacity would sit idle in between spikes, but with sharing, that capacity can be used to provide commercial services, making the approach highly cost-effective [4]. In addition, given the potentially high cost of meeting capacity demands of a

once-in-a-decade spike, priority roaming gives public safety access to more capacity than would otherwise be realistically possible. The capacity gains from roaming are particularly great in cases where not all transmitters are collocated. For example, a device transmitting at 100 kb/s near the edge of a cell might consume the same resources as a device transmitting at 400 kb/s near the center, and a device located at cell edge in the public safety network might be in the center of a cell in a commercial network. Thus, if public safety systems are designed such that devices near the cell edge are more likely to roam than those near the cell center. Thus, for example, merely tripling the amount of spectrum public safety can access in an emergency may lead to an order of magnitude increase in capacity.

In addition to the capacity benefits, priority roaming also increases system resilience. When mobile devices are able to roam from one network to another, then they can operate even if one network fails. For example, after the 9/11 attacks, the communication system used by police in the World Trade Center continued to function, as did several commercial networks, but the system used by firefighters failed, leaving them unable to communicate [1]. Many inside the World Trade Center probably never heard the orders to evacuate as a result [1, 31]**.** In circumstances like these, priority access and roaming could save lives.

## 6. Innovative ways to reduce costs by working with commercial cellular providers

Public safety wireless networks and commercial cellular networks today share no infrastructure in almost all cases. Figure 3 below shows the physical architectural elements that are candidates for sharing. Figure 4 below shows the logical network architectural elements for sharing. Figure 5 provides more detail for the elements at a cell site. The elements in a network that are candidates for sharing include the cell sites, the antennae on the towers, the cabling, the radio processing equipment at the tower, the power systems, the common processing equipment, the high speed backhaul from the cell site to the core network, the core network infrastructure, and the servers and ancillary systems the define the services, administrative features, customer/officer profiles, and other operations support systems. In general, the amount of sharing could potentially range from the extreme of no sharing today to complete sharing of the all physical assets in an 4G wireless network. That is, in the advanced IP world of the future, different service or logical networks could share a physical infrastructure and, in effect, be separate logical Virtual Networks on the same shared physical network.

*Exhibit 4-V: Illustrative Wireless Network Architecture*

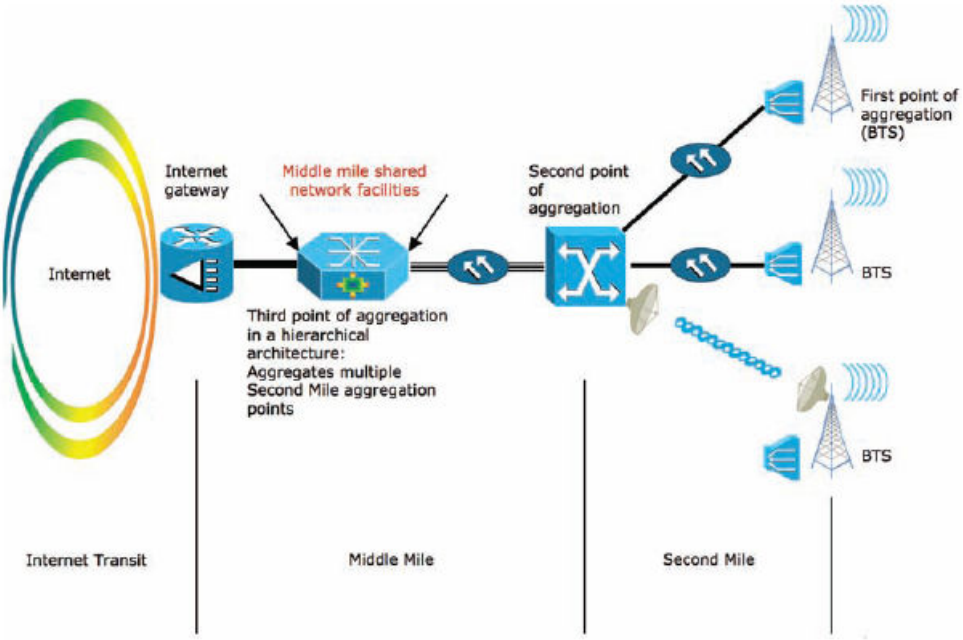



Figure 3

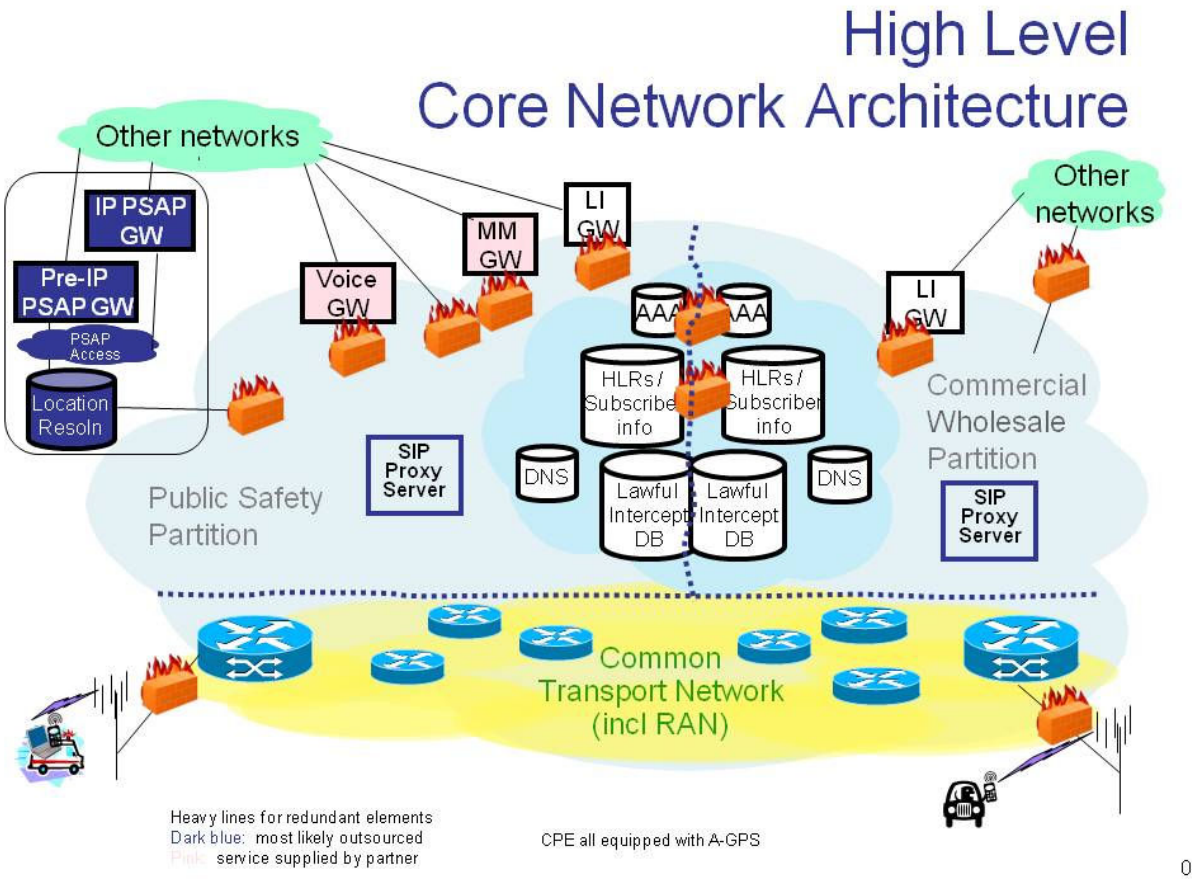
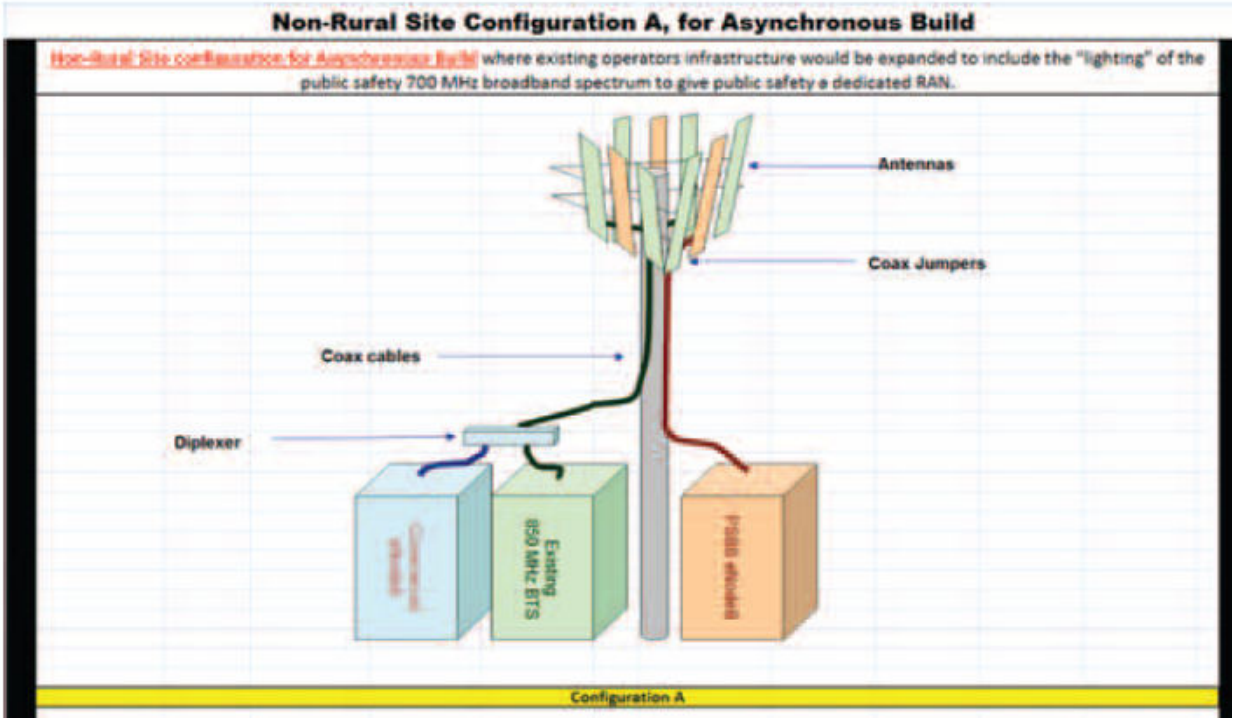



Figure 4


Non-Rural Site Configuration A, for Asynchronous Build
Non-Rural Site configuration for Asynchronous Build where existing operators infrastructure would be expanded to include the "lighting" of the public safety 700 MHz broadband spectrum to give public safety a dedicated RAN.
Antennas
Coax Jumpers
Coax cables
Diplexer
Existing 850 MHz BTS
PSBB eNodeB
Configuration A

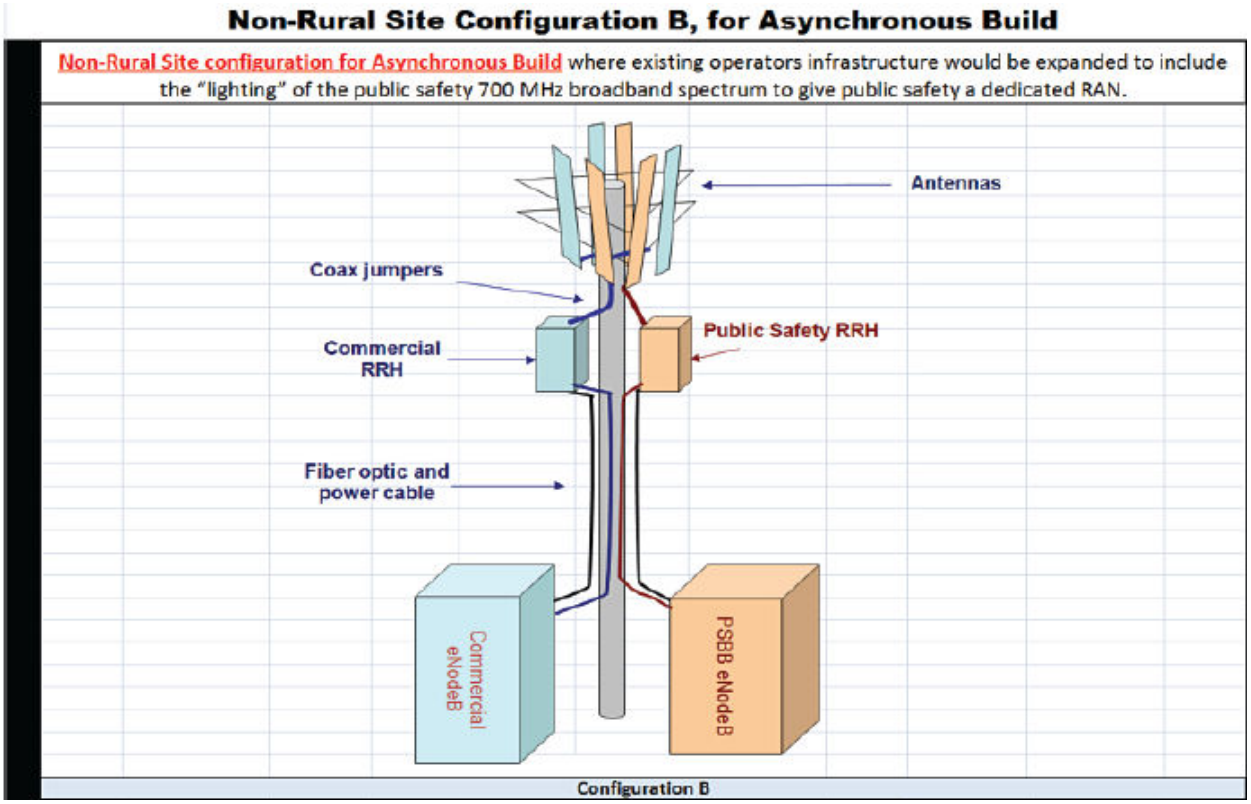

Non-Rural Site Configuration B, for Asynchronous Build
Non-Rural Site configuration for Asynchronous Build where existing operators infrastructure would be expanded to include the "lighting" of the public safety 700 MHz broadband spectrum to give public safety a dedicated RAN.
Antennas
Coax jumpers
Commercial RRH
Public Safety RRH
Fiber optic and power cable
Commercial eNodeB
PSBB eNodeB
Configuration B

Figure 5

The NBP recommendation is to share cell sites, power systems at the cell sites, some common processing equipment, and the backhaul from the cell site to the core network and the core network. Public safety would have dedicated spectrum and radio access equipment for their primary use and dedicated ancillary services and administrative services that defined their unique services and command and control structures including authorization, authentication, and security. The NBP did not mandate this approach, but it did assume this approach when estimating costs, and the savings were substantial. This section will go further into the advantages of the approach.

As explained in Section 5, the FCC estimated that between 40,000 and 45,000 cell sites will be needed to provide the type of service and quality of service that public safety agencies will be required. That is almost as many cell sites as Verizon or AT&T have – and they support 80 to 100 million users. Public safety agencies only have between 1 and 3 million users authorized under current statutes to use this spectrum, and the actual number of first responders in the field using mobile communications is likely less. To support a nationwide network of more than 40,000 sites for a user base of only a few million is costly from both opex and capex standpoints. This would be analogous to building a separate limited access highway systems just for police cars and fire trucks. Therefore to provide a network that can meet the coverage requirements of public safety and support the performance requirements, particularly for uplink incident video, there is good reason to pursue cost sharing opportunities with commercial assets.

The OBI Technical Paper No. 2, "A Broadband Network Cost Model" [27] provides the detailed analysis of the cost of building and operating a network that leverages commercial assets as described above. The total capex costs for this build is $6.5 B consisting of

- $4.0 billion to equip 41,600 commercial towers with dedicated public safety broadband spectrum RAN capabilities;
- $1.5 billion to harden the commercial towers (improving reliability, particularly when commercial power is lost);
- $0.8 billion to equip 3,200 rural towers with public safety broadband spectrum RAN capabilities by upgrading towers (75%) and installing and equipping new towers (25%)and hardening those towers; and
- $0.2 billion to provide for a fleet of public safety deployables (a mix of next generation COWS, COLTS, etc.), vehicular area network systems and non-recurring engineering costs for handset development.

The cost model also estimated the total on-going opex at $1.3 B per year in the $10^{th}$ year consisting of:

- 0.9 billion for IP Managed Services and Transport including backhaul and core from commercial operators exclusive of opex for the public safety RAN;
- $0.2 billion for Managed Services for the dedicated public safety RAN;
- $0.2 billion for additional ongoing costs for rural areas (microwave backhaul, additional site lease cost, etc.); and
- $0.025 billion for operations support for deployable equipment.

By contrast, as discussed in the Cost Model Technical Paper [27], a stand-alone network that did not leverage commercial infrastructure would require at least 2.5 times more capex, excluding deployable equipment, and proportionally even more in ongoing costs.

The leverage of commercial assets provides both public safety and the commercial networks a more robust infrastructure cost effectively, thereby providing a synergistic benefit for both parties. Most cell sites and all of the core infrastructure of commercial networks are connected by resilient fiber rings that continue to operate in the face of a single failure such as a fiber cut. Installing such fiber rings for a new stand-alone public safety infrastructure would be prohibitively expensive. Today, one of the most common points of failure for public safety networks is the single backhaul link from the tower site to the core network. This failure likelihood would be greatly reduced since the partnership approach enables public safety to inherit the benefit of the fiber rings. In turn, the hardening of the commercial cell sites, the funding of which would be provided under the NBP, provides the commercial operator partner with a more robust network. This in turns benefits the public welfare since the restoration of commercial cellular infrastructure in the face of major disasters such as hurricanes and large scale terrorist events is critical to public safety.

Another major additional advantage of this incentive partnership approach is the much more rapid build-out of the nationwide public safety wireless broadband infrastructure. The major cellular operators will be building out LTE networks over the next few years. As one example, Verizon has stated that it is committed to building out LTE in the 700 MHz spectrum to over 95% of American citizens by 2014. [33] So the public safety broadband infrastructure could be built out at the same time as the LTE build-out. Moreover it is likely that the LTE build-out will use the existing cell site and backhaul assets that the cellular operators already have.

## 7 Governance and Network Management

One of the key issues that arise as you construct a new network for public safety communications is how to ensure that network is truly interoperable. Because public safety communications networks must be developed to serve a variety of needs, it is imperative that from the start a framework is developed to ensure that nationwide interoperability is created. Failure to ensure interoperability from the start of a network may mean added cost and technical complications in the future.

The FCC's recommendations would meet these needs in a number of ways. One is in the recommended approach to funding. As discussed in greater detail in Section 6, the NBP recommended total funding of $12 to $16 billion for the nationwide public safety network. In the past, public safety funding has come from a variety of sources. Under the NBP strategy, a single federal agency would be responsible for distributing the federal contributions to this network, ensuring a higher degree of consistency and facilitating long-range planning.

NBP recommendations also included the creation of an Emergency Response Interoperability Center (ERIC). ERIC was deemed as necessary to ensure that no matter if there was one licensee or many, that the network would be interoperable. Past experience has shown not

having a common interoperability framework leads to fragmented networks. ERIC, which has been established as a part of the FCC, has the critical function of creating a technical framework for interoperability of the nationwide broadband network. ERIC will achieve this by establishing a common technical framework and working through difficult issues of roaming and priority access, security and encryption, among others. Of course it is critical that public safety have a voice in the development of this framework, so in addition to standard notice and comment provisions, the FCC has established a Technical Advisory Committee and is also establishing a public safety advisory committee to ERIC. Further, to ensure interoperability is also achieved with federal partners, ERIC has established a relationship with various federal partners to receive their input.

However, to ensure that the technical framework that is developed is complied with, it is imperative that these requirements become license conditions and also are conditions of any grant funding that is received by a public safety network operator. Failure to have incentives to comply with technical and imperative requirements has in the past led to non-compliance.

ERIC is already hard at work establishing initial interoperability requirements based on public comment it has recently received. These include setting air interface requirements and minimum performance capabilities. Further, ERIC is currently examining the interoperability showings filed by waiver recipients for early builds of the public safety broadband network. Further, ERIC is working very closely with the Public Safety Research Lab at the National Institute of Standards and Technology (NIST) to best understand the technologies that public safety will utilize in its network and how to ensure interoperability. In this regard, NIST has a unique role as they can analyze how technologies best support public safety.

While ERIC is an important step, other federal agencies, such as the Department of Homeland Security and the Department of Justice are critical to work with public safety to ensure the governance procedures are in place to ensure interoperability. Each agency has a special role in the United States process and their expertise is valued in these discrete areas. These agencies will need to move forward to quickly work with public safety and develop standard operating procedures and other governance principles to ensure that the public safety broadband network is interoperable on day 1.

By establishing a framework from Day 1 of the public safety broadband network it is likely that the nation will be successful at ensuring that the public safety broadband network is truly interoperable across geographies and agencies. Failure to achieve this may lead to increased cost for interoperability and network fragmentation. To this end, it is very important that the FCC examine the best way to allow usage of the public safety broadband spectrum to ensure that the fragmentation that has occurred in the past does not occur in this context. Therefore, in the near term, the FCC will further explore this issue.

There is a great opportunity here to avoid the interoperability mistakes of the past. By utilizing consumer electronic based technologies, where interoperability has been available for years, and balancing the special needs of public safety, public safety by working with ERIC and other federal partners, will, for the first time, have the opportunity to deploy and operate a truly nationwide interoperable communications network.

## 8 Conclusions

The nation's First Responders need a modern evolving interoperarable nationwide wireless broadband infrastructure to support state-of-the art data, video, and multi-media communications from times of normal operations to times for dire emergencies and even wide spread devastation. This infrastructure must be cost-effective to build out and affordable to operate. Connecting America: The National Broadband Plan [5] recommended a multi-faceted public safety broadband infrastructure that leverages commercial technology and commercial assets as a complement to a dedicated Radio Access infrastructure for public safety in order to achieve a cost effective approach for the tax payer. The plan includes both funding recommendations and importantly new governance and administrative practices to ensure the long-term health and interoperability of public safety communications.

The multi-Faceted approach to robust anywhere anytime communications is provided through:

- a hardened Radio Access Network infrastructure with dedicated spectrum designed to public safety's strict requirements to enable a high degree of coverage, signal reliability, and resilience
- priority roaming on commercial 4G network to provide access to additional capacity during emergencies, as well as increased network resiliency
- in-building and underground solutions to provide superior coverage
- deployable technology for vehicles to provide coverage where none exists because of failures or remoteness, and to provide enhanced capabilities for major incidents.

Cost effectiveness is achieved through:

- the use of technology based on commercial standards, in particular 4G LTE, ruggedized for public safety, which will reduce costs and fuel innovation in the equipment used for public safety communications
- incentive-based partnerships, which allow public safety to leverage commercial infrastructure in a new and cost-effective manner
- the use of commercial networks assets, e.g. tower sites, backhaul, redundant fiber rings, where feasible

By adopting a nationwide approach, and leveraging widely available technologies and commercial assets, the NBP recommendations for public safety will save taxpayers billions of dollars, providing the high-performance broadband capabilities that public safety agencies need at far lower costs than would be possible with dedicated assets and equipment built only for public safety. At the same time, by providing funding and governance structures focused on ensuring dependable and interoperable communications capabilities throughout the nation, the NBP recommendations will provide public safety with better communications than would be possible if they relied only on commercial providers.

Effective governance is achieved through:

- Institutional arrangements that bring consistency and interoperability, allow all parties to be heard, and provide incentives to reduce costs and increase efficiency
- A new entity, the Emergency Response and Interoperability Center, which will ensure interoperability across networks, now and as the networks evolve over time.
- Funding grants with very specific compliance requirements

The NBP for public safety recommended $12 to $16 B of funding to provide the U.S. first responders with the 21st century interoperable wireless broadband infrastructure they need and deserve.

**Acknowledgements**
The authors would like to thank Jason Kim and Kim Anderson for their assistance with this draft. The authors would like to recognize the work of the FCC Technical Team for their extensive work on the NBP recommendations on the nationwide interoperable public safety network. The team includes Pat Amodio, Behzad Ghafari, Brian Hurley, Kurian Jacob, Walter Johnston, John Leibovitz, Tom Peters, Ziad Sleem, Jerome Stanshine, and Joon Yang.

**References**

[1] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report,* 2004.

[2] Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, Report and Recommendations to the Federal Communications Commission, June 12, 2006.

[3] J. M. Peha, "How America's Fragmented Approach to Public Safety Wastes Spectrum and Funding," *Proc. Telecommunications Policy Research Conference,* Sept. 2005. Expanded version in *Telecommunications Policy*, Vol. 31, No. 10-11, Nov. 2007, pp. 605-18. www.ece.cmu.edu/~peha/safety.html

[4] R. Hallahan and J. M. Peha, "Quantifying the Costs of a Nationwide Broadband Public Safety Wireless Network," *Proc. 36th Telecommunications Policy Research Conference,* Sept. 2008. Expanded version to appear in *Telecommunications Policy.* www.ece.cmu.edu/~peha/safety.html

[5] Federal Communications Commission, *The National Broadband Plan: Connecting America,* March 14, 2010. www.broadband.gov

[6] Federal Communications Commission, Second Report and Order, "In the Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010," WT Docket No. 96-86, August 2007.

[7] Federal Communications Commission, Office of Inspector General, Report, D-Block, Investigation, http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-281791A1.pdf, April 25, 2008

[8] R. Hallahan and J. M. Peha, "The Business Case of a Nationwide Wireless Network that Serves both Public Safety and Commercial Subscribers," *37th Telecommunications Policy Research Conference (TPRC)*, Sept. 2009. www.ece.cmu.edu/~peha/safety.html

[9] Department of Homeland Security, National Emergency Communications Plan, July 2008, http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf

[10] TETRA Association, *TETRA vs. P25*, March 2007. http://web.mac.com/warrenhavens/iWeb/Site/TETRA%20vs%20P25.html
[11] "Motorola Brute i680: Ultra-Rugged With Noise Cancellation," *About.com:Cell Phones*, August 16, 2010 .http://cellphones.about.com/od/motorolacellphonereviews/fr/motorolabrutei680.htm
[12] Federal Communications Commission, Wireless Competition Report, "In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993 Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services" pg. 170, "Average Price After Discount for PDAs/Smartphones and All Handsets", May 20, 2010. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-81A1.pdf
[13] CCID Consulting: Demands and Technology Drive Growth of China's Mobile Phone Market, August 4, 2008. http://www2.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/08-04-2008/0004860897&EDATE=
[14] Donny Jackson, Public Safety Groups Support LTE at 700, *Urgent Communications*, June 11, 2009. http://urgentcomm.com/networks_and_systems/news/700-mhz-lte-support-20090611/
[15] "APCO & NENA Endorse LTE as Technology Standard for the Development of Nationwide Broadband Network," *APCO News,* June 9, 2009 , http://www.apco911.org/new/news/nena_endorse_lte.php
[16] NPTSC, National Public Safety Telecommunications Council Press Release: NPSTC Votes To Endorse LTE Technology for Broadband Network, June 10, 2009. http://www.npstc.org/documents/Press_Release_NPSTC_Endorses_LTE_Standard_090610.pdf
[17] 3GPP, "The Mobile Broadband Standard: 3GPP Features and Study Items", http://www.3gpp.org/ftp/Specs/html-info/FeatureListFrameSet.htm, August 16, 2010
[18] 3GPP, "The Mobile Broadband Standard: Releases" August 16, 2010. http://www.3gpp.org/releases and http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/
[19] U.S. DEPARTMENT OF JUSTICE, Integrated Wireless Network, http://www.usdoj.gov/jmd/iwn
[20] Federal Communications Commission, Second Further Notice of Proposed Rulemaking, "In the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band," PS Docket No. 06-229, May 2008.
[21] J. M. Peha, "Fundamental Reform in Public Safety Communications Policy," *Federal Communications Bar Journal,* vol. 59, no. 3, pp. 517 – 546, June 2007. www.ece.cmu.edu/~peha/safety.html
[22] Michelle Farquhar on behalf of Lemko, *Ex Parte* Presentations GN Docket No. 09-51,, http://ecfsdocs.fcc.gov/filings/2010/02/25/6015538923.html, February 25, 2010
[23] Michelle Farquhar on behalf of Lemko, *Ex Parte* Presentations, GN Docket No. 09-51, Nov. 4, 2009. http://fjallfoss.fcc.gov/ecfs/document/view?id=7020244821
[24] Brian Ponte, on behalf of Lemko, *Ex Parte* Presentations, GN Docket No. 09-51, Dec. 22, 2009. http://fjallfoss.fcc.gov/ecfs/document/view?id=7020354555
[25] Phil Weiser and Dale N. Hatfield, "In Pursuit of a Next Generation Network for Public Safety Communications," *CommLaw Conspectus - Journal of Communications Law and Policy*, Vol. 16, No. 1, 2007.

[26] National Public Safety Telecommunications Council, Public Safety 700 MHz Broadband Statement of Requirements , Federal Communications Commission Docket 07-114, 2007.
[27] Federal Communications Commission, A Broadband Network Cost Model, A Basis for Public Funding Essential to Bringing Nationwide Interoperable Communications to America's First Responders, May 2010. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-297709A1.pdf
[28] Federal Communications Commission, The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost, June 2010. http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0615/DOC-298799A1.pdf
[29] Department of Homeland Security, SAFECOM Program, Public Safety Statement of Requirements for Communications & Interoperability Volume I (2006) and Volume II (2008).
[30] New York City Department of Information and Technology, Federal Communications Commission Docket 07-114, Nov. 17, 2009.
[31] Jim Dwyer and Kevin Flynn, *102 Minutes*, Times Books, 2006.
[32] J. Marsh, "Secondary Markets in Non-Federal Public Safety Spectrum," *Proceedings of the Telecommunications Policy Research Conference*, Sept. 2004.
[33] Dick Lynch, Wireless Telecommunications Symposium, Keynote Speech Tampa, FL**,** April 22, 2010. http://www22.verizon.com/NROneRetail/NR/rdonlyres/61AD27CC-91C7-43BB-A81D-DD1978408C31/0/DL_WTS_042210v6.doc