THE BENEFITS OF TRANSITIONING TO A NATIONWIDE WIRELESS BROADBAND NETWORK FOR PUBLIC SAFETY

JUNE 2011

The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety

At a recent hearing before the Senate Commerce Committee, New York City Police Commissioner Raymond Kelly remarked that a 16-year-old with a smartphone has "more advanced communications capability than a police officer or deputy carrying a radio."[1] The failings of public safety communications systems include both interoperability—with the limitations of current systems becoming tragically apparent on 9/11 and in the aftermath of Hurricane Katrina[2]—and operability—with the cost-effectiveness and performance of traditional public safety devices trailing well behind those provided by modern commercial cellular operators.

With the emerging rollout of commercial services marketed as 4G, LTE-based wireless services, there is a once-in-a-generation opportunity to transform the effectiveness of our first responders through a national strategy to develop and deploy a nationwide wireless broadband network for public safety. Such a broadband service promises to enhance the effectiveness of public safety agencies and, if developed appropriately, can also ultimately replace their legacy (and very expensive) communications infrastructure and devices.

This report explains how the President's Wireless Innovation and Infrastructure Initiative can facilitate the transition away from the traditional, fragmented world of public safety communications to a next generation system. It begins by providing the relevant context, explaining, among other things, the drawbacks of today's systems, and it concludes by discussing benefits and opportunities made possible by a successful transition to an LTE-based nationwide network. In so doing, it recognizes that this transition will take some time and, in order for it to be successful, it must planned carefully, coordinated effectively, and begin as soon as possible.

I. The Legacy of Land Mobile Radio Systems and the Rise of the Modern Cellular Industry

Public safety agencies were the original pioneers of wireless technology. Indeed, public safety's use of Land Mobile Radio ("LMR") services dates back almost a century.[3] The Detroit Police Department, for example, used an early form of LMR in 1921, experimenting with a one-way (base-to-vehicle) system.

1. Police Commissioner Raymond W. Kelly: Testimony on "Safeguarding Our Future: Building a Nationwide Network for First Responders," U.S. Senate Committee on Commerce, Science, & Transportation, at 1 (Feb. 16, 2011) *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=04981480-8117-4289-905d-c1498aa72ee1.

2. *The 9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* (July 22, 2004), *available at* http://www.gpoaccess.gov/911/Index.html; "The Federal Response to Hurricane Katrina: Lessons Learned" (Feb. 2006), available at http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf.

3. This historical discussion is drawn from Dale N. Hatfield, *The Technology Basis for Wireless Communications, in* THE EMERGING WORLD OF WIRELESS COMMUNICATIONS 49 (1996).

Based on the technology available at the time, systems like this one used Amplitude Modulation ("AM") located in the frequency range just above the AM broadcast band. Later, public safety agencies began to use systems in the Very High Frequency ("VHF") band, using the more effective Frequency Modulation ("FM") band.

Over time, as public safety communications technology advanced, the FCC authorized new spectrum allocations for these services. In the mid-1970s, for example, the FCC allocated additional spectrum in the 800 MHz band for private LMR (including public safety entities), making spectrum available not only for the traditional and conventional, single-channel dispatch systems described above, but also "multi-channel trunked systems."[4] Building on the increasing interest in developing such systems and encouraging "interoperability" among them, the public safety community launched a standards development effort that evolved into the Project 25 Initiative (P25).[5]

While the P25 effort made progress in facilitating greater levels of interoperability among first responders, there remains no national, interoperable LMR network and equipment costs remain very high. Several challenges hindered the progress of the P25 effort. Notably, over a decade after P25 got moving, the GAO concluded that "ambiguities in the published standards [for the Project 25 initiative] have led to incompatibilities among products made by different vendors, and no compliance testing has been conducted to ensure that vendors' products are interoperable…As a result, state and local agencies have purchased fewer, more expensive radios, which still may not be interoperable and thus may provide them with minimal additional benefits."[6] Since that GAO report, the Federal government has created a compliance assessment program for P25 equipment, and while successful, the program has limitations based on the level of industry participation and standards development progress.

Beyond P25 specifically, the lack of better-coordinated public safety communications reflects two basic historical facts. First, as a general matter, first responders are supported by state and local revenue bases and have always bought equipment from their own local budgets. As such, efforts to improve interoperability involved the difficult work of coaxing agencies that traditionally operated on their own to begin working with one another. Second, because for decades public safety was forced to provision its own services, public safety communications grew up in an environment in which being a "smart controller" of services provided by another entity was not an option. In the modern broadband world, by contrast, public safety agencies are generally not operating their own networks. They either procure such services from commercial providers (such as Verizon or Sprint) or they contract with a vendor to operate a network on their behalf (as Northrop Grumman has for New York City).

Over the last 25 years, the modern cellular industry has expanded exponentially. By the late 1980s, the commercial cellular industry was just beginning to outgrow the public safety community in terms of size and significance as a user of wireless technologies. From around 340,000 U.S. subscribers in 1985,

4. An Inquiry Relative to the Future Use of the Frequency Band 806-960 MHz; and Amendment of Parts 2, 18, 21, 73, 74, 89, 91, and 93 of the Rules Relative to Operations in the Land Mobile Service Between 806 and 906 MHz, *Second Report and Order,* 46 F.C.C. 2d 752, ¶¶ 16-17 (May 1, 1974).

5. Telecommunications Industry Association, Project 25, Public Safety Communications Interoperability—Frequently Asked Questions Available on TIA Web Site, PulseOnline, Oct. 2004, http://pulse.tiaonline.org/article.cfm?id=2057.

6. U.S. Gov't Accountability Office, First Responders: Much Work Remains to Improve Communications Interoperability 4 (2007).

commercial wireless grew nearly tenfold over the next 25 years, reaching over 300 million subscribers in 2010. Public safety, however, has largely continued to use wireless services outside this evolving commercial ecosystem. As such, it has failed to benefit from the economies of scale and the ongoing innovation that has taken place in that sector.

II. A Next Generation Public Safety Communications System

The success of the modern cellular industry has enabled its users to reap enormous benefits in operability—including ongoing innovation and cost-performance capabilities—and interoperability—where all users can access one another (for both voice and text communications). The requirements for public safety differ from commercial wireless users, however, making conventional commercial services generally unsuitable for public safety's mission-critical communications.

The traditional LMR systems and devices developed for public safety have served public safety agencies well with regard to meeting their unique requirements. Most notably, such systems are developed to provide rapid voice call-setup and group-calling capabilities. (Ordinary cellular systems, by contrast, can allow for seconds to go by before a call is delivered and answered.) When time is of the essence, as is often the case when public safety agencies need to communicate, it is important to have access to systems that achieve fast call-setup times. Similarly, unlike ordinary cellular systems, dispatch systems like those used by public safety allow for large talk groups to communicate either among individual units or by broadcast messages (think: "calling all cars").

Above and beyond rapid call-setup and group-calling capabilities, public safety agencies also depend on a number of other important functionalities. Most notably, public safety relies on devices that allow for a handset feature known as "talk-around," which enables two or more mobile or portable units to communicate without the aid of network infrastructure. In the case of emergency situations where such infrastructure is not available, a peer-to-peer mode of communications is crucial. Similarly, modern public safety dispatch networks provide queuing and priority access capabilities that traditional cellular networks were not designed to provide. In short, despite their operability and interoperability limitations, traditional LMR systems have provided public safety agencies with mission-critical capabilities that conventional cellular systems have not generally offered. These systems will continue to be essential for public safety communications until broadband systems are able to meet public safety requirements, particularly for mission-critical voice.

While maintaining their traditional LMR systems, public safety agencies are increasingly using commercial broadband systems to support their missions. Such agencies are adopting modern broadband systems in different shapes and forms, including using laptop computers in vehicles, as secondary communications devices (e.g., a smartphone), or for remote video monitoring. In many cases, agencies have relied on commercial off-the-shelf services. In some cases, jurisdictions have procured services directly, such as New York City's relationship with Northrop Grumman to build and operate a broadband wireless network.[7]

7. Press Release, Northrop Grumman, Northrop Grumman Wins $500 Million New York City Broadband Mobile Wireless Contract (Sept. 12, 2006), *available at* http://www.it.northropgrumman.com/pressroom/press/2006/pr31.html.

The development and deployment of LTE systems represent a new opportunity for public safety communications. For starters, public safety can develop and deploy a nationwide network that will enable greater levels of operability and interoperability in the mobile broadband arena than public safety has ever achieved in the world of traditional LMR systems. Moreover, this opportunity holds the promise of public safety systems that could be developed based on commercial standards to generate significant economies of scale, competition in equipment as well as services, and ongoing innovation of the kind experienced in the modern cellular industry. With the move to LTE, public safety can seize this very opportunity.

Given the growth of commercial services, the opportunity to leverage such assets promises to make the development and deployment of an LTE wireless broadband network for public safety far less expensive than it would if public safety were to own and operate such a network itself. In 1991, such a model (with less than 10,000 sites nationwide) was far from appealing. By contrast, the situation in 2011 (with more than cell sites in service) makes this a compelling opportunity.

The challenges of using commercial infrastructure are not dissimilar to those of adapting the commercially developed LTE standard and ordinary services to meet the requirements of public safety. In particular, public safety communications systems must be survivable and able to function in the midst of a natural or man-made disaster. To that end, such systems require a degree of "hardening" and back-up power capability that can ensure that they are available during times of emergency. As with the development of lower cost devices, the opportunity to use infrastructure that can be shared between public safety and other users can greatly lower the cost for public safety communications. Notably, basic infrastructure—towers, high capacity lines, and electricity costs—can be shared in an environment where public safety has its own spectrum and network that meets its particular needs.[8] And as Part III explains, the President's Wireless Initiative provides a framework to make such a network possible.

III. The President's Wireless Initiative and Public Safety Communications

In his 2011 State of the Union address, President Obama announced his Wireless Innovation and Infrastructure Initiative,[9] specifically referencing the opportunity for a firefighter to use a handheld device to download the floor plans of a building before arriving at the scene of an emergency. Such technology, which could enhance the effectiveness of our first responders, is routinely used by enterprises like Federal Express to enhance their mission.[10] For our first responders, however, the best they can do in the current environment is to adopt ad hoc solutions based on commercial technology. Given the appropriate federal leadership, public safety can shape the development of emerging broadband solutions to specifically meet its needs, thereby providing a transition path away from its legacy equipment and networks.

8. Access to back-up satellite systems might well be another requirements for certain public safety systems, insofar as such a capability provides another backup network as well as an ability to communicate in remote areas.

9. The White House. "President Obama details plan to win the future through expanded wireless access." February 2011. http://www.whitehouse.gov/the-press-office/2011/02/10/president-obama-details-plan-win-future-through-expanded-wireless-access.

10. Hamblen, Matt. "FedEx to adopt rugged handhelds from Motorola." *Computerworld*. September 2009. http://www.computerworld.com/s/article/9138071/FedEx_to_adopt_rugged_handhelds_from_Motorola.

As President Obama outlined, the Wireless Initiative pays for itself and would reduce the deficit by enabling more efficient use of wireless spectrum and by freeing up spectrum for auction. This initiative catalyzes investment and innovation in the wireless broadband ecosystem by freeing up 500 MHz of spectrum over ten years through more efficient federal government and private sector use of this resource. This effort is expected not only to drive investment and innovation, but also to generate almost $28 billion in revenue. Obtaining such revenue, for which President Obama has reserved almost $10 billion in his 2012 Budget for deficit reduction, depends on Congress acting to authorize the FCC to conduct "voluntary incentive auctions" as well as an updated framework to facilitate the more efficient use of government spectrum (i.e., an update of the Commercial Spectrum Enhancement Act).

After using the proceeds from spectrum auctions to reduce the deficit, President Obama proposed four related measures to spur investment and innovation in next generation wireless technologies for public safety purposes. In two related steps, President Obama called for an investment in a nationwide wireless network for public safety communications based on 4G technology, and for the rollout of 4G services to at least 98% of the American population. These two steps are related because the construction of 4G services to otherwise unserved parts of the country will enable both public safety agencies to use those services and for citizens living in those areas to obtain service. Third, President Obama called for the D Block, which is a band of spectrum in the 700 Megahertz band that is required to be auctioned, to be reallocated for public safety. Finally, President Obama has championed the creation of a Wireless Innovation (WIN) Fund that would, among other things, support investments in research that would enable LTE-based technology to meet the particular requirements of public safety for mission critical data, voice, and video.

For the core commitments of President Obama's plan to be realized, Congress will need to address the relevant funding, technology, and governance issues that will enable a nationwide network for public safety to be developed and deployed.

Developing an effective nationwide public safety governance structure will be crucial to ensuring that public safety has access to a network with far greater levels of operability and interoperability than it has ever had before. A key part of this effort is moving away from the traditional path of individual jurisdictions making isolated purchasing decisions on equipment, devices, and services. Under that legacy model, the equipment and infrastructure were generally costlier, open standards that enabled public safety to support an innovation ecosystem (such as an "apps store" for public safety) did not exist, and even neighboring systems (or sometimes even communications systems within the same jurisdiction, such as fire and police) could not interoperate. Absent a governance system that will drive standard setting activity and ensure that local purchasing decisions support interoperability, there is a strong possibility that we will repeat the mistakes of LMR in the wireless broadband arena.

The management of wireless broadband network development and deployment requires an effective and empowered nationwide governance system. In particular, developing nationwide wireless broadband services tailored for public safety will require a national body that can specify the requirements for public safety communications, hold the license for public safety broadband spectrum, and oversee a competitive bidding process to enlist the best providers that can develop, deploy, and operate the appropriate wireless broadband system. Such a body should be composed of highly competent professionals, including leaders in the field of public safety, information technology, and cellular communications networking, operations, and deployment.

The continued development of effective regional, statewide, and local governance mechanisms is similarly critical to enabling the effective use of a wireless broadband network developed for public safety. In particular, such mechanisms ensure that the control over the network—including what agencies have priority in what circumstances—is exercised in a well coordinated fashion and is responsive to end user needs. Moreover, such mechanisms provide a basis for identifying key local issues with respect to coverage and opportunities for sharing infrastructure.

IV. The Opportunity for Cost Savings and Enhanced Effectiveness from a Nationwide Next Generation Public Safety Communications System

The development and deployment of a nationwide public safety next generation network promises significant opportunities for long term cost savings and improved functionality. While there are considerable initial Federal budgetary costs to establish a nationwide network, they will be offset in the medium and long run by three primary sources of savings: (1) reduced government spending focused on overseeing and managing today's fragmented and inefficient networks; (2) savings from reduced device and infrastructure costs; and (3) innovation enabled by competition and market entry as public safety adopts a modern wireless standard.

Even more important than the money saved, the Nation's first responders and public safety agencies will, on account of this initiative, be safer and more effective because they will have at their disposal a wealth of new devices, applications, and other cutting-edge technology. From accessing video images of a crime in progress, downloading building plans of a burning building to a handheld device, or connecting rapidly and securely with personnel from other towns and cities, a nationwide wireless broadband network for public safety will make a difference on a day-to-day basis—and not merely during the most severe emergencies when the availability of an interoperable and operable network will be at its most important.

A. The benefits from achieving a fully interoperable system

First and foremost, developing and deploying a nationwide wireless broadband system provides a unique opportunity to develop and deploy a network that is interoperable by design. The benefit of interoperability by design is difficult to capture as an economic matter because its value is in the more effective emergency response capability that results from those at the scene of an incident enjoining seamless and easily managed communications networks. It is also difficult to capture the costs of the assorted interoperability measures now being used, ranging from swapping radios to using Internet-based gateways to patch together non-interoperable systems.[11] In short, not only would interoperability be effectively achieved at the network level—providing our first responders with a greater level of effectiveness—but it would be achieved far more cost-effectively than today's solutions allow.

11. It merits note that such measures will continue to be used for the reasonably foreseeable future in that the transition to an LTE-based interoperable environment that replaces today's legacy LMR systems may well take a decade. Moreover, during this transition period, it will be important for LTE systems to have a level of backward compatibility to legacy LMR systems.

B. The benefits from a coordinated system for public safety communications

Today's public safety communication systems not only lack some of the capabilities of modern networks and commercial devices, but the systems are also fragmented across thousands of Federal, State, and local jurisdictions. This fragmentation puts the responders—and the public—at risk in emergencies like 9/11 or Hurricane Katrina, when different law enforcement agencies could not talk to one another. But beyond reducing the effectiveness of our public safety officials, this fragmentation also adds to the cost of communications systems, reducing resources for governments at every level. As one commenter explained:

> Particularly since 9/11, there has been great concern about the possibility of failures due to lack of interoperability, and failures due to a shortage of public safety spectrum. This paper shows how both of these and other serious problems are a logical consequence of America's fragmented approach to public safety, in which thousands of local agencies make independent decisions without a coherent strategy to unify or guide them. Because of this fragmented approach, public safety agencies build more infrastructure than they should, spend more taxpayer money than they should, and consume more scarce spectrum than they should, all for a system that is unnecessarily prone to interoperability failures.[12]

In general, the costs of maintaining this fragmented system are borne by Federal, State, and local governments. On the Federal front, DHS will award over $2 billion in grants for preparedness and homeland security as part of the FY2011 Budget, with many of the programs supporting communications procurement. Moreover, in a one-time infusion in 2007, the joint NTIA/FEMA Public Safety Interoperable Communications Grant program awarded $968 million to fund interoperable communications in 56 States and Territories.[13]

These costs to the Federal government—and the expenses incurred by State and local agencies—could be reduced substantially through the economies of scale gained by transitioning to a nationwide, interoperable network. An analysis of several different approaches concluded that the costs of this transition would be paid for in reduced spending towards the current, fragmented network within several years:

> Given the tremendous inefficiencies of the current fragmented system, as demonstrated above, it is perhaps no surprise that the cost of building an entire nationwide system is comparable to what is likely to be spent in just a few years to upgrade and maintain the existing infrastructure. For example, in the wake of 9/11, the U.S. federal government has dispersed billions of dollars in grants just to address communications issues at the state and local level, and billions more will be needed. In fact, the cost to upgrade the entire existing infrastructure has been estimated at $18 billion. In contrast, we found

12. Peha, Jon M. "How America's fragmented approach to public safety wastes money and spectrum," 33rd Telecommunications Policy Research Conference (September 2005), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1029&context=epp&sei-redir=1#search="peha+waste+money+public+safety+communications.

13. Department of Commerce. National Telecommunications and Information Administration. "Public Safety Interoperable Communications (PSIC) Grant Program." Accessed May 2011. http://www.ntia.doc.gov/psic/index.html.

that deploying a single 700MHz nationwide network that carries voice and data will cost about $10 billion.[14]

In addition to savings on Federal grants, one of the very significant benefits and opportunities from the President's plan is to provide federal first responders with the opportunity to use this network. It will require, however, just the sort of network—with the intelligent control capabilities of an advanced network—discussed herein to provide such users with the capabilities and assurances they need. To ensure that the public safety network is built to meet the requirements not only of public safety, but also Federal first responders, the Emergency Communications Preparedness Center is in the process—under the leadership of DHS—of developing an assessment of their broadband communications requirements.

C. Savings through economies of scale on devices and infrastructure

As it stands today, there are more than 2 million first responders in the Federal, State, and local governments.[15] This includes nearly 300,000 firefighters, more than 630,000 police patrol officers, and countless other public safety workers such as forest fire inspectors, correctional officers, and security guards. The Federal government, moreover, employs around 100,000 individuals in protective service occupations. Many of these public servants rely on advanced communication infrastructure and devices to go about their jobs every day. For our Federal, State and local governments, extra spending on communications devices comes directly out of the budget used to hire and retain police officers, fire fighters, and other first responders—not to mention education, healthcare, road maintenance, and other public services. Once it is fully implemented, the President's plan will allow governments at all levels to save on communications device and infrastructure costs, leaving more resources for State and local governments to improve public safety and other services.

The cost difference between traditional devices used by public safety and commercially available ones is quite stark. As a recent Congressional Research Service report found, "the latest radios developed for public safety…cost between $4,000 and $6,000. The current narrowband radios being used for 700 MHz networks typically start at $3,000."[16] By contrast, commercially-available 4G smartphones cost around $600.[17] To be sure, as explained above, this is not an apples-to-apples comparison. Although commercial smartphones have some functions that go beyond public safety communications devices—think of Internet-enabled applications available on such devices—they lack the ruggedness, reliability, rapid calling and conferencing, and direct device-to-device connectivity of traditional LMR systems and equipment. Consequently, a core part of the President's initiative focuses on developing the necessary technology based on the LTE standard to meet the requirements of public safety, enabling public safety to use commercially-developed handsets.

---

14. Hallahan, Ryan and Jon M. Peha. "Quantifying the costs of a nationwide public safety wireless network." Working Paper. Carnegie Mellon University. Accessed May 2011. http://www.andrew.cmu.edu/user/rhallaha/papers/quantifying_costs_of_PS_network.pdf.

15. U.S. Department of Commerce. Bureau of the Census. Occupational Employment Statistics. National Occupational Employment and Wage Estimates by Ownership. Protective Service Occupations. May 2009 (most recent available). http://www.bls.gov/oes/current/999001.htm.

16. Moore, Linda K. "Public safety communications and spectrum resources: Policy issues for Congress." Congressional Research Service. September 2010. http://www.fas.org/sgp/crs/misc/R40859.pdf.

17. M. Maesto, "Apple Selling Unsubsidized Phones for $500-700: Report," *available at* http://www.eweek.com/c/a/Mobile-and-Wireless/Apple-Selling-Unsubsidized-iPhones-for-500-to-700-Report-682945/.

Once the relevant requirements are built into public safety systems based on 4G technology, end user devices for such systems are expected to be between five and ten times less expensive than today's LMR technology. As the Congressional Research Service concluded, "The participation of commercial carriers in developing and deploying, for example, a common radio interface, is expected to put the cost of public safety radios in the same price range as commercial high-end mobile devices ($500)."[18] Similarly, an analysis by Andrew Seybold concluded that "the overall cost savings will be substantial and we believe that the industry is willing to work with the public safety community to provide the types of devices it requires at reasonable costs."[19]

With respect to savings on infrastructure, public safety communications systems that leverage existing commercial (and governmental) infrastructure can be cost effective. Similarly, using greater leverage in procuring devices that are used across a national network also promises considerable cost savings. In examining this issue recently, the FCC found that leveraging available commercial systems could save considerably on capital expenditures compared with relying on the existing public safety communications infrastructure.[20]

D. Providing better performance and cost effectiveness through innovation

Public safety communications will benefit from a broader market for devices and technology, overcoming the fragmentation of today's often-proprietary systems and improving interoperability through non-proprietary, open standards of commercial wireless technology. Participation in a broader market based on open standards will also allow public safety to enjoy the benefits that come from many more firms competing to offer goods and services. Not only will devices and infrastructure be upgraded and improved based on advances in commercial technology, but public safety's adoption of an Internet-based framework will enable developers to provide open and standards-based applications for public safety use. To facilitate this opportunity, the President's plan calls for clear, nationwide standards that make public safety systems interoperable across jurisdictions and vendors.

Government Accountability Office findings support the fact that the lack of an open standards and a commercially vibrant ecosystem constitutes a critical weakness in public safety communications.[21] Further, a recent Federal Communications Commission letter to the Chairman of the House Committee on Energy and Commerce describes how clear, nationwide standards have the potential to rectify the poor performance currently experienced in public safety.[22] In particular, the FCC explained "the beneficial effect of competition through open standards" as follows:

---

18. Federal Communications Commission. Letter to the Honorable Henry Waxman. July 20, 2010. http://democrats.energycommerce.house.gov/documents/20100726/Letter.FCC.07.26.2010.pdf.

19. Seybold, Andrew. "Comments on the FCC White Paper: Federal Communications Commission Omnibus Broadband Initiative." April 2010. http://andrewseybold.com/1572-white-paper-response-to-fcc-white-paper.

20. FCC. OBI Technical Working Paper No. 2. "A broadband network cost model: A basis for public funding essential to bringing nationwide interoperable communications to America's first responders." May 2010. http://download.broadband.gov/plan/fcc-omnibus-broadband-initiative-(obi)-technical-paper-broadband-network-cost-model-basis-for-public-funding-essential-to-bringing-nationwide-interoperable-communications-to-americas-first-responders.pdf.

21. GAO. "First Responders: Much work remains to improve communications interoperability." April 2007. http://www.gao.gov/new.items/d07301.pdf.

22. Federal Communications Commission. Letter to the Honorable Henry Waxman. July 20, 2010. http://democrats.energycommerce.house.gov/documents/20100726/Letter.FCC.07.26.2010.pdf.

> P25 systems still rely upon proprietary solutions and the beneficial effect of competition through open standards is not fully realized. A comparison to Tetra, a European standard similar to P25 but which was successfully completed in 1995, makes this stagnation clear. Though similar in function to P25, Tetra products are both more spectrally efficient than P25 and significantly cheaper…A broad framework for interoperability is essential to ensuring that this network is interoperable from day one and remains so as the technology evolves.

The former Los Angeles Chief of Police testified that modern broadband networks for public safety would allow law enforcement to deploy a range of innovative new technologies: "Today, many agencies have established Real Time Crime Centers that are leveraging new technologies to do an even more effective job of fighting crime…New technologies such as automated license plate readers, biometrics, medical telemetry, automated vehicle location, and streaming video only scratch the surface of the capabilities that will be carried by broadband networks."[23] Similarly, New York City Police Commissioner Raymond Kelly reiterated the importance of modernizing public safety communications in Congressional testimony in February:

> [An effective broadband network] could provide officers with an immediate, digital snapshot of anyone they detain. It would give them the suspect's address, prior arrest history, and other critical details. The officer would be able to take electronic fingerprints at the scene and compare them instantaneously with those in local, state, and federal databases. This kind of situational awareness is vital to the safety of the officers and members of the public.[24]

The testimony above clearly demonstrates public safety communications' need for nationwide, interoperable, open, standards-based voice and data broadband networks to replace the legacy public safety systems in use today. Of the many benefits a nationwide broadband network could enable, perhaps the most critical is to improve situational awareness and provide the opportunity for comprehensive identification.

In a public safety setting, accurate information about the subject, the surrounding area, and the environment is critical. Law enforcement and other public safety practitioners make better and more informed decisions when interacting with the public if they can access comprehensive identification and databases containing a range of information (e.g., driver's licenses or other photos; records of warrants, arrests, prison time, school attendance, or history of violent behavior; and customs and immigration status). Even current information with respect to weather or environmental concerns such as flood plains and wind direction can improve a practitioner's ability to do an effective and efficient job. But all of this information—pictures, records, video, etc.—requires bandwidth and the technology necessary to deliver such information to a handheld device. As explained above, that technology does not need to be invented, only tailored to meet the needs of public safety.

---

23. Bratton, William. Testimony Before the House Committee on Energy and Commerce Subcommittee on Communications, Technology, and the Internet. September 2009. http://democrats.energycommerce.house.gov/Press_111/20090924/bratton_testimony.pdf.

24. Kelly, Raymond. Testimony before the Senate Committee on Commerce, Science, and Transportation." February 2011. http://pdf.911dispatch.com.s3.amazonaws.com/senate_hearing_d-block_feb2011.pdf.

One example of comprehensive identification and improved situational awareness is the use of license plate readers. Public safety is quickly recognizing the value of license plate reader (LPR) technology in both the fight against crime and the battle against terrorism. LPRs are used in fixed, portable, and mobile environments to check against a defined alert lists for wanted status.[25] These lists may be combined or customized as needed and may include thousands of plate numbers at any given time. Checking vehicle status via LPR can be done hundreds, even thousands, of times in a single shift. Without LPRs, a patrol officer determines wanted status by either manually entering a plate via an in-car computer system or requesting the check by radio. Recognizing a wanted vehicle solely by observation relies on memory or reference to a printed list called a "hot sheet." Since LPR checks require little to no action on the part of the officer, full attention can be given to other tasks, such as driving or looking for crimes in progress, making the entire process much more effective while enhancing public and officer safety.

No matter how the data transport is achieved, the available bandwidth to provide the connectivity is critical to the performance of the system. Although some agencies still rely on manual flash drive updates at shift changes to update LPR systems, many are moving to wireless connectivity (3G, 4G, WiFi, and satellite) to improve the timeliness of data uploads. Fixed and portable LPRs may have the benefit of wired connectivity for updating data, but increasingly are dependent on wireless connectivity because LPRs tend to be installed in remote locations or areas lacking fixed infrastructure.

Another example of comprehensive identification and improved situational awareness is the dramatic increase in both use and value of streaming video to and from emergency vehicles in the field. A doctor at a hospital, with real-time broadband data communication with an enroute rural ambulance crew, might more swiftly recognize a patient's symptoms, and be able to give instructions to the ambulance crew resulting in potentially better life-saving treatment. (Also see Appendix A).

In-car video can also be useful in providing visual information to mobile command posts and emergency operations centers in the event of a major incident. As an example, a patrol officer responding to a structure fire can provide real-time visual assessment of the structure and provide specific information relevant to proper response that an individual patrol officer may not even be aware is relevant to fire personnel. This provides incident command staff and emergency operations much better situational awareness and understanding as input to command decisions, and as in the previous example, much more rapid and appropriate response to evolving situations.

Conclusion

The President's Wireless Initiative promises to both improve public safety's effectiveness and reap savings by providing public safety with a state-of-the-art nationwide wireless broadband system. Such a system will finally enable it to benefit from economies of scale of commercial infrastructure and devices as well as ongoing competitive innovation in that ecosystem. As such, the ultimate savings and benefits from this transition are very likely to eclipse and more than compensate for the upfront investment in a nationwide, modern broadband network. Most importantly, this effort will provide public safety officials

25. An LPR takes a photo of the license plate using a Smart Phone or Tablet PC camera and runs a check against a defined list. *See* Appendix A.

with access to a modern communications network that will enable them to better protect themselves, our families, and homeland security.

Appendix A

Examples of Innovative Applications for Public Safety Broadband

1. **License Plate Reader**
   By taking a photo using a smartphone or Tablet PC's camera, the investigator can automate the process to capture the license plate information to determine if the car is stolen and its registered owner. Not only can the photo be stored, but information such as location and date/time can be useful intelligence.

2. **Fingerprint Identification**
   Through M2M technologies tethered to the smartphone of Tablet PC, the fingerprint of a subject can be collected and searched against Law Enforcement databases to quickly identify a person and assess the level of threat incorporating the existing capabilities from Quick Capture Platform (QCP) and Repository for Individuals of Special Concern (RISC). QCP enables the mobile identification and enrollment using a mobile system. RISC enables rapid search to quickly assess the level of threat within seconds with two to ten fingerprint images in a mobile environment.

3. **Facial Recognition**
   By taking a picture with a smartphone or Tablet PC's, a subject's photograph can be matched against existing databases such as the DMV or booking databases to determine identity.

4. **Scars, Marks, and Tattoos**
   By taking a picture with a smartphone or Tablet PC's camera, a symbol can be matched against existing databases to determine identity, relationships, and intelligence such as symbol affiliation, last time seen, contributing department/agency, etc.

5. **Field Interview Cards**
   After conducting a field interview, an investigator can enter the information in a timely manner without the need to return to the office. The investigator can also query the database for relevant data on previous interviews.

6. **Crowd Sourcing and Interactive Maps**
   In multi-agency operations such as the Inauguration and Super Bowl, crowd sourcing applications along with interactive maps enhance situational awareness by providing real-time data and gathering intelligence through geo-location aware services.

7. **Local, State, Federal Data**
   Various apps with the ability to query Local, State, and/or Federal databases will provide investigators the ability to selectively search the appropriate repositories and return the right amount of information in a timely manner. This also applies in the EMS field.

8. **Child Abduction Leads Tracking**
   To expedite law enforcement response in Amber alert cases, integration of leads tracking functionality into Virtual Command Center will facilitate leads assignments and investigator updates in the field environment. Geographic information system (GIS)/visual-based icon-driven

situational awareness and common operating picture user interfaces connecting operational data bases.

9. **Multi-vital sign patient data transmission and access to patient history,** including real-time multi-vital sign data, current patient status (medic notes in real time), and high-definition video (patient and imaging video and stills, e.g., CT and ultrasound) regardless of location (e.g. emergency department, incoming helicopter, incoming back-up ambulance(s)).