Emergency Response Interoperability Center
Public Safety Advisory Committee (PSAC)

Considerations and Recommendations for Evolution of the Public Safety Wireless Broadband Network

PSAC Network Evolution Working Group Report

May 24, 2011

Acknowledgements

The following individuals contributed to the creation of this report:

Kenneth C. Budka, Alcatel-Lucent, Chair
Paul Steinberg, Motorola Solutions, Vice Chair
Kenneth Boley, Designated Alternate, National Association of State Chief Information Officers (NASCIO)
Donald Brittingham, Designated Alternate, Verizon Wireless
William Brownlow, American Association of State Highway and Transportation Officials (AASHTO)
Alex Coleman, Verizon Wireless
Patricia Cooper, Satellite Industry Association (SIA)
Adel Ebeid, National Association of State Chief Information Officers (NASCIO)
Tom Goode, Alliance for Telecommunications Industry Solutions (ATIS)
Doug Mah, Washington State Department of Information Services
Brant Mitchell, State of Louisiana
Steve Noel, State of Oregon
Mark Poulin, Designated Alternate, Motorola Solutions
Andrew Seybold, National Sheriffs' Association
Steve Sharkey, Designated Alternate, T-Mobile, USA
Bradley Stoddard, State of Michigan, Michigan Public Safety Communication System
Tom Sugrue, T-Mobile, USA
Gary Wingrove, National EMS Management Association (NEMSMA)

Table of Contents

1 Executive Summary

An important element of the Federal Communications Commission's (FCC's)[1] policies surrounding development of a nationwide public safety wireless broadband network is establishment of a network evolution framework that will enable public safety officials to leverage the technological advancements that regularly occur in the wireless industry. In doing so, the FCC provides greater assurance that Emergency Response Providers will have access to the most advanced communications capabilities possible and that the nationwide public safety wireless broadband network will keep pace with innovations occurring in the private sector.

1.1 Summary of Recommendations

Based on the deliberations of the Network Evolution Working Group to date[2], we make the following recommendations:

1. A tiered governance framework is needed to allow for orderly evolution of the public safety wireless broadband network. The governance structure must adjudicate interoperability issues on a national basis, and, as appropriate, delegate sufficient autonomy to regional entities (e.g., states, UASI regions, etc.) to implement the evolution plan.

2. Network evolution must consider early (waiver) deployments and accommodate them into the nationwide network. These pioneer networks constitute important opportunities for learning and technical advancement. In addition, the field experience gained in the planning, deployment, and operation of these networks will help inform future network evolution decisions. Thus, it is important that these networks are able to deploy with confidence that they will not be stranded so long as they adhere to current and future regulations and guidelines, in particular those related to adherence to standards.

3. The risks intrinsic in adopting new commercial technology must be balanced with the benefits realized from the associated capabilities provided. Given the nature of their mission and the dependence upon technology in life and death situations, public safety will likely not be early adopters of new technology; however, it is imperative that the public safety wireless broadband network keeps pace with the commercial industry to the extent possible in order to continue to accrue the benefits of leveraging commercial technology. To successfully evolve the public safety wireless broadband network and maintain nationwide interoperability, public safety must be sufficiently funded on a perpetual basis. On-going investment is needed to keep the nationwide network and devices current relative to commercial technology.

4. Application considerations that should be factored into the network evolution plan include the following to the extent that the noted capability is leveraged in the public safety network:

[1] A complete list of acronyms is provided in section 9.

[2] The Network Evolution Working Group held its first meeting on March 15, 2011.

a. Many public safety agencies have currently deployed wireless data applications running on top of commercial wireless data services. In the commercial world, such applications are known as “Over the Top Applications,” referring to their ability to run on top of a best-effort IP data service without requiring additional integration effort. Such applications are already being used by public safety on commercial networks, and thus can be readily used on the public safety wireless broadband network. Support for over the top applications can be significantly enhanced through the introduction of priority services or other supplemental security services that are required by public safety.

b. Applications that require access to quality of service features, network features, e.g., evolved Multimedia Broadcast Multicast Service (eMBMS), or additional services, e.g., Public Switched Telephone Network (PSTN) voice, Short Message Service-Multimedia Message Service (SMS-MMS) messaging that require additional equipment that may not be part of an initial LTE network deployment

c. SMS-MMS Messaging support and underlying implementation, e.g., IP Multimedia Subsystem (IMS)

d. Land Mobile Radio (LMR) Gateways (Note: Standards have yet to be completed to support this functionality).

e. Long Term Evolution (LTE) geo-location service

f. One-to-Many Communications across All Media (as eMBMS Service is not yet available)

g. PSTN Voice (as devices and device capabilities and network capabilities for this capability will be developed over time)

h. LMR Voice (Support of LMR-like voice service over an LTE network will require support of quality of service, LTE’s eMBMS and other features. Dual-mode devices supporting both an LTE interface and an LMR interface will be required, with the LMR interface providing talkaround service and direct access to Project 25 (P25) and conventional networks when LTE coverage is not available. To ensure nationwide interoperability, open standards must be developed to support LMR voice over LTE.)

5. Public safety should review the commercial standards specification in conjunction with vendors and network operators to determine a feature/function set which best suits public safety.

a. Once a governance group is put into place, regulators should not mandate any of the LTE standards as network requirements; rather, this should be left to the standards bodies and the public safety wireless broadband network governance group. The network governance group should not permit the deployment of proprietary solutions that in any way prevent or inhibit interoperability. The public safety wireless broadband network governance group should, in contemplating network evolution, consider early (waiver) deployments and accommodate them into the evolution of the nationwide network. Such accommodation must be done in a way that does not compromise interoperability.

b. Regulators should alert the public safety wireless broadband network governance group of any proposed rules and requirements and secure this group's approval before the rules and requirements are enacted.

6. Public safety will need to determine what new capabilities it will leverage for its applications, plan an introduction roadmap, and also ensure that as the network evolves, uses of earlier technology is not compromised and interoperability maintained. This primarily affects balancing four aspects: Application to Application, Device to Network, Network Element to Network Element, and Network to Network. Not all of these items are addressed purely by standards.

7. As the network is built out, it is expected that it will incrementally expand to increase geographic coverage. As regional networks "grow" together, it will be important for the evolution to take into account a cohesive RF plan and interconnect strategy.

8. Capacity planning must be coordinated between regional portions of the network and shared national components to ensure that the entire network scales end-to-end. Due to the costs associated with buildout (support of higher data rates results in increased costs), it is inadvisable for the FCC to mandate minimum supported rates/performance unilaterally across all networks and locations within the networks.

9. As the network topologically evolves (sites are added, cores are added, etc.), overall consideration of network resiliency has to be continually evaluated. Resiliency has to be applied at the regional level to ensure that each such deployment is robust. Resiliency also must be incorporated on a national scale for network assets that are truly operated nationwide (e.g., an IP backbone used to interconnect regional deployments).

10. As new security threats come into being and additional/improved methods to secure information are devised, best practices and response to real time threats should be coordinated nationally.

11. A comprehensive public safety network evolution plan must be developed and maintained. This network evolution plan will be a living document, reviewed periodically and updated to reflect changes in technology, user requirements, field experience and other factors. The network evolution plan must ensure that interoperability is maintained as the network evolves. A network evolution plan makes the evolution of the network explicit to all stakeholders, and enables coordinated rollout and evolution.

1.2 Items for Further Study

The Network Evolution Working Group has identified the following areas as items for further study and recommends that the FCC convenes future working groups to address these topics as time allows and in relative order of priority of need and impact.

1. Develop specific recommendations for a governance framework that ensures nationwide interoperability while allowing for orderly build out and coordinated evolution of the public safety wireless broadband network.

2 Charter and Approach

2.1 Charter

The Public Safety Advisory Committee (PSAC) was established as a Federal Advisory Committee chartered to provide recommendations to the FCC regarding best practices and actions the Commission should undertake as part of its rule making initiatives aimed at implementation of the public safety wireless broadband network.[3]

The Public Safety Advisory Committee is comprised of four working groups focused on the following topics:

- Interoperability
- Applications and User Requirements
- Security and Authentication
- Network Evolution

The Network Evolution Working Group is comprised of 14 members, including a Chair and Vice Chair. In addition, 4 designated alternates periodically filled in for four of the PSAC members. The Commission selected the Network Evolution Working Group membership from among the members of the full PSAC.

The Network Evolution Working Group was tasked with providing recommendations based on the following question:

"How to establish network requirements that will ensure evolution?"

2.2 Approach

Commercial wireless and other technologies that comprise the nationwide public safety wireless broadband network will evolve over time as new features and functionality are added, and new technological innovations are developed and adopted by the marketplace. Public Safety's requirements for the nationwide public safety wireless broadband network will also change over time, shaped by

[3] *See* 75 Fed. Reg. 43164 (2010).

evolving mission needs, experience and experimentation with new applications, existing capabilities of the network, the anticipated benefits of new technologies and other factors.

The mission of the Network Evolution Working Group is to develop recommendations for the public safety wireless broadband network to help ensure the United States' Emergency Response Providers are able to effectively, and in a cost efficient manner, take advantage of new technologies in a way that best supports public safety mission requirements and sustains nationwide interoperability.

The evolution of the public safety wireless broadband network will be primarily driven by two interrelated and somewhat interdependent factors: system needs and user needs. User needs describe what the public safety wireless broadband network needs to do in order to provide a foundation for support of public safety applications. System needs describe what the public safety wireless broadband network needs to do in order to meet operational goals.

User Needs
Application Foundation
System Needs
Operational Goals

Public safety network evolution will be driven by a number of factors.

- **Technology Evolution:** To help develop recommendations for public safety wireless broadband network evolution, the Network Evolution Working Group studied the factors driving evolution of commercial LTE networks, network evolution best practices used by commercial service providers, the evolution of LTE standards and equipment, and the impact of network evolution on the support of public safety applications. By adopting LTE, public safety will become part of the broader LTE ecosystem. Understanding the evolution of LTE and the LTE ecosystem are essential parts of planning for the evolution of the public safety wireless broadband network. Such understanding will help public safety best take advantage of the new functionality provided by LTE while helping mitigate the risks associated with technological evolution.

- **User/System Needs:** In anticipation of the deployment of public safety wireless broadband networks, public safety organizations have begun to specify the types of applications that they wish to be supported. To help develop recommendations for public safety wireless broadband network evolution, the working group studied how support of different public safety wireless broadband applications would impact network evolution.

Members of the Network Evolution working group come from a diverse set of backgrounds: representatives of public safety agencies, representatives of commercial service providers, and representatives of LTE equipment providers. The recommendations in this report were developed through discussion (working group conference calls and email exchanges) and reached in unanimity.

3 Network Evolution: the Commercial Wireless Carrier Perspective

Commercial wireless carriers have years of accumulated experience in planning the evolution of large, complex wireless networks across multiple generations of technology. As such, aspects of the best current practices commercial wireless carriers have adopted for the evolution of their networks can help guide the evolution of the public safety wireless broadband network.

The evolution of commercial wireless networks involves the participation of all members of the commercial wireless ecosystem. Commercial wireless service providers continually work with technology developers, equipment manufacturers, and others to develop technological advancements that provide greater value for wireless consumers. A number of factors drive the development and adoption of these new technologies, including:

- Network performance
- Spectral efficiency and network capacity
- Network costs
- Performance and costs of devices
- Ability to support non-traditional wireless applications, and
- Availability and suitability of spectrum

These factors are discussed in more detail in the following sections. Each is an important consideration in making decisions about technological development and network evolution.

3.1 Network Performance

A principle goal in deploying any broadband technology is improved customer performance in the form of increased throughput. This is a key factor in the decision by wireless service providers to deploy LTE, as LTE enables substantially higher network throughput (approximately ten times that supported by existing 3G technologies) through the use of wider RF channel bandwidths and advanced modulation and coding techniques. While increased throughput is an important technology driver, it is not the only factor that influences decisions about broadband technology. Another key factor in the decision to deploy LTE is its ability to substantially reduce latency (network delay). Lower latency is critical for real-time, interactive commercial applications such as video and voice conferencing, mobile gaming, and peer-to-peer applications. These features are also essential to public safety applications, where real-time response and situational awareness are critical. Other important performance factors include: LTE’s ability to support converged voice, data, and video services; support of global roaming; and enablement of “one-to-many” and “many-to-many” communications. In short, LTE more closely approximates the performance characteristics of wire line broadband technologies than previous generation wireless technologies.

3.2 Spectral Efficiency and Network Capacity

Spectral efficiency, the measure of the amount of user traffic that can be carried in a block of spectrum, has always been an important technology driver for commercial carriers. Spectral efficiency has direct impact on network costs: the more spectrally efficient a technology, the higher the amount of data that can be carried in the spectrum licensed to a commercial operator (network capacity).

The explosive growth of commercial wireless data and multimedia services has made spectral efficiency even more critical. Increased spectral efficiency and new allocations of spectrum increase the data carrying capacity of each base station. This increase in base station capacity allows wireless service providers to absorb this explosive traffic growth without requiring explosive growth in the number of base stations they deploy. The use of Orthogonal Frequency Division Multiple Access (OFDMA) for mobile broadband networks, for example, was an important development. OFDMA enables LTE networks to make more efficient use of spectrum. Other factors that affect network capacity include the use of advanced antenna technologies (e.g., MIMO)[4] and the use of smaller cell sites (e.g., femtocells).[5]

3.3 Network Costs

Utilization of more advanced and more spectrally-efficient network equipment has always been an effective means to decrease network costs, while also increasing network capacity. The development and widespread adoption of these technologies based on a common set of uniform standards is also effective at facilitating global scale and driving down the cost of network equipment.

A key technology driver of LTE has been the emergence of a flat, all-IP architecture. LTE's flat, all-IP architecture lowers network costs in two ways. First, the architecture reduces the number of network elements in the data path compared to legacy technologies, lowering operations costs and capital expenses. Second, the support of voice, video and data services on a common network will eventually allow wireless carriers to retire legacy, voice-centric technologies. The retirement of legacy technologies, so-called "planned obsolescence," is a commercial wireless carrier best practice: legacy technologies are retired when the costs of maintaining them no longer justify the benefits, where "benefits" are measured in economic terms: lower capital expenditures, lower operations costs, and higher revenues. In addition to reducing costs, planned obsolescence allows the spectrum occupied by legacy technologies to be re-used for other purposes.

There is an additional benefit of lower network costs, lower latencies, and higher capacities: the combination of these factors enables wireless broadband services to be more competitive from a price/performance perspective with wired networks.

3.4 Performance and Costs of Devices

Wireless devices are no longer limited to cell phones and simple data devices. There has been a virtual explosion in the type and number of wireless devices. As a result, the proliferation of connected devices (e.g., cameras, monitors, asset trackers, etc.) is a key consideration in the decisions that service providers make about technology and network evolution. In addition to the incorporation of more advanced radio technologies, device manufacturers must leverage advances in underlying components

[4] Multiple-input multiple-output (MIMO) transmission employs multiple antennas at the transmitter and receiver to improve communications performance.

[5] Femtocells are small cellular base stations, often deployed indoors, that can help to improve coverage as well as increase network capacity through improved spectrum reuse. In addition to improving network capacity, the use of femtocells can also help to reduce capital and operating expenses.

such as screens, processors, and RF components. These advancements are critical to enabling a higher level of performance at costs that are sustainable for the mass market. Two key goals of LTE operators and device manufacturers are promoting uniform standards that facilitate global scale and enabling a broad ecosystem that will promote wide-scale development of applications for LTE devices. Development of security measures to protect the network and the consumer (e.g., unauthorized uses, malicious attacks, etc.) will also become increasingly important.

3.5 Non-Traditional Wireless Applications

While broadband technologies will enable traditional wireless applications to be more robust, a key driver for deployment of LTE is its ability to support of host of new applications and services that have not traditionally been provided over commercial wireless networks. This includes areas like consumer electronics, machine-to-machine, medical devices, telemetry, energy management, mobile commerce and security. Just as new applications are finding their way onto commercial networks, it is expected that public safety applications which have not yet been contemplated will also find their way onto the public safety wireless broadband network as the network is built and put into operation.

3.6 Spectrum Considerations

Access to sufficient spectrum is, of course, a critical consideration that impacts network performance, capacity and cost. Spectrum allocations are needed that will support the new technologies being developed and promote global harmonization. Technologies like LTE that promote scalable bandwidths enable operators to make most efficient use of available spectrum. Service provider network evolution plans take into account changes in the carrier's spectrum assets.

4 Public Safety Network Evolution Governance Assumptions

As is apparent from the discussion in the previous section, wireless carriers balance many factors over different time horizons when planning and orchestrating the evolution of their networks. To manage this process, wireless carriers typically maintain an organization responsible for establishing network evolution plans and corresponding execution strategies. It is therefore reasonable to assume that a comparable function is needed in the overall governance structure of the nationwide public safety wireless broadband network.

This section outlines major assumptions regarding such a structure that would be necessary to orchestrate public safety network evolution. In general, we assume that a tiered governance structure would be applied with "national" and "regional" (e.g., states, UASI regions, etc.) planes. The national level would optimally delegate as much as possible to the regional level and retain jurisdiction at the national level over those areas that are essential to ensure nationwide interoperability and resolve issues which cannot be addressed at regional levels. In adopting such a structure, care must be taken to ensure that regional decisions do not adversely affect other regions or compromise the functionality, costs and evolution of the nationwide network. While it is beyond the scope of this document to make specific recommendations on the make up and overall purview of such a governance entity, we have identified this as a crucial area for efficient and effective evolution of the public safety wireless broadband network. Thus, we propose to treat this as an item for further study and recommend that the FCC convenes future working groups to address these topics as time allows.

a. Part of the governance body has the on-going role of making decisions about the evolution of the public safety wireless broadband network. These decisions will have implications on each regional segment of the network, the national network as a whole, users of the network, funders of the network, the costs of supporting future applications on the network, ease of network operations, and other factors. To make informed decisions, the body should consider a wide scope of input, including, for example, the current state of commercial wireless deployments, new public safety application and mission requirements, support of functionality not present in commercial networks[6], the costs of supporting new network functionality, the effect of network evolution on existing deployments and nationwide interoperability, adherence to high-volume commercial open standards, and other factors. Many of these evolution decisions require deep understanding of the underlying technology. Many of the decisions on public safety applications needs require deep understanding of public safety operations. Because of the wide spectrum of factors impacted by evolution decisions, evolution decisions are often not cut and dry. Study teams with appropriate experts can be commissioned to analyze particular topics/subjects and considerations effecting the Network Evolution Plan. Ultimately, network evolution decisions must be adhered to by all public safety agencies. Failure to do so can compromise interoperability. Compliance will help ensure nationwide interoperability and, furthermore, help harness the economic power of public safety agencies to influence the LTE ecosystem.

b. An arm of the governance group should develop and maintain a uniform nationwide architecture for the public safety wireless broadband network that identifies the guiding principles of the network's evolution, detailed requirements for interoperability, and a roadmap for support of applications.

c. An arm of the governance group should be responsible for budgeting and monitoring the costs of network deployment and ongoing operations. One essential factor in network evolution decisions is overall impact on costs. Such decisions should be informed by current experience. This may include determining how costs should be allocated among the different entities that comprise the nationwide network related to network evolution.

d. An arm of the governance group should be responsible for establishing minimum performance criteria and on-going measurement and monitoring network performance. Network performance is a driving factor in network evolution.

e. An arm of the governance group must ensure that backward compatibility and interoperability is maintained as the network evolves. Backward compatibility and interoperability must be designed in as part of the network evolution process. As the network evolves, new functionality must be carefully tested to ensure backward compatibility and interoperability are not compromised.

[6] For example, new functionality needed to support network management and coordinate QoS and preemption among different user classes.

f. An arm of the governance group must ensure that disputes between entities are satisfactorily resolved. Unresolved disputes over time undermine the authority of the governance body, potentially compromising network evolution (and interoperability).

g. The governance structure and policies must consider early (waiver) deployments and accommodate them into the evolution of the nationwide network. These pioneer networks constitute important opportunities for learning and technical advancement in addition to creating useful feedback that inform future decisions. Thus, it is important that these networks are able to deploy with confidence that they will not be stranded so long as they adhere to current and future regulations and guidelines.

h. A comprehensive public safety network evolution plan must be developed and maintained. This network evolution plan is a living document, periodically reviewed and updated to reflect changes in technology, user requirements and other factors. The network evolution plan must ensure that interoperability is maintained as the network evolves. A network evolution plan makes the evolution of the network explicit to all stakeholders (public safety agencies, vendors, commercial service providers, etc.) and enables coordinated rollout and evolution. Making the evolution of the network explicit helps align the LTE ecosystem, reducing the research and development risks faced by developers of network equipment and user devices, and promoting competition and innovation.

5 Public Safety Application Considerations

LTE supports a rich set of broadband communications features. Using LTE, for example, video, high resolution images, and other multimedia data can be exchanged among public safety personnel in the field, backend systems and support personnel. Access to real-time multimedia information over LTE can be used to quickly establish a common operating picture among different teams responding to an emergency. This common operating picture can allow incident commanders to better plan and execute a coordinated emergency response, enhancing public safety and the safety of Emergency Response Providers. In addition, using LTE, public safety personnel in the field can access and provide data to database systems, a significant tool in enhancing the effectiveness and safety of day-to-day operations and planned events. The ability to operate in the field, in a mobile environment, for day-to-day operations, as well as unplanned events with the same capabilities that normally would have been only available in a brick and mortar facility, are the real advantages of LTE to help evolve public safety with the use of technology.

There is a strong interdependency between network evolution and the applications that can be supported over the public safety LTE network. As new features are incorporated in the LTE network, existing applications will be enhanced and new applications and tools will be developed to take advantage of these features. In addition, the desire to deploy new applications supported by new LTE releases, user devices, and network infrastructure is one of the factors that will drive evolution of the public safety wireless broadband network. Understanding the benefits, costs, and risks of supporting different applications and the requirements applications place on the LTE network, devices and backend systems and the timeframes in which different applications can be supported is an essential part of developing a network evolution plan.

In anticipation of the deployment of commercial broadband technologies in the US Public Safety 700 MHz band, the National Public Safety Telecommunications Council (NPSTC) convened a Broadband Task Force. This Broadband Task Force, comprised of representatives of public safety agencies, service providers and equipment vendors, developed a set of minimum recommendations necessary to ensure roaming and interoperability among Regional LTE broadband Systems that various Public Safety entities were planning.

The NPSTC Broadband Task Force issued a report[7] which included a list of "required" and "desired" applications. "Required" applications were those the Task Force recommended be supported on networks constructed under FCC waiver. "Desired" applications were those the Task Force determined were "recommended but not required and may not be technically supported for early build out of regional networks." As such, desired applications will be a factor in the evolution of networks constructed under waiver.

As additional source material on application requirements for the broadband public safety network, the U.S. Department of Justice Office of Community Oriented Policing Services (the COPS Office), along with the U.S. Department of Homeland Security and U.S. Department of Commerce, hosted the National Forum on Public safety wireless broadband Needs in Washington, D.C., August 19–20, 2010. This forum convened key participants from the public safety practitioner community to help identify, discuss, and develop solutions and recommendations that will help accurately reflect public safety's operational and business requirements for a National Public Safety Wireless Broadband Network.[8] This document provides useful insights into the operational requirements that must be achieved.

To help illustrate the need for and benefits of network evolution, the PSAC Network Evolution Working Group decided to use the NPSTC Broadband Task Force's list of required and desired applications and examine their impact on network evolution (and vice versa). Some of the applications specified by the Task Force can be successfully supported with the IP data service provided by equipment built to the initial release of the LTE standard (Release 8). These so-called "over-the-top" applications can operate with adequate user-perceived performance without the need for additional network features. Their operation, however, can be enhanced as the network evolves through the provision of priority service features which may or may not be available in early network deployments.

To support transmission of voice or video with adequate end-to-end performance, applications must be able to signal the quality of service requirements of different data streams. Additionally, the network must ensure proper handling of packets throughout the network to satisfy quality of service requirements. Further, support of cellular-like voice services will require the deployment of additional

[7] "NPSTC 700 MHz Public safety wireless broadband Task Force Report and Recommendations," September 4, 2009. (http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf)

[8] "National Forum on Public safety wireless broadband Needs," August 23, 2010. (http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf)

network infrastructure to support call handling, interoperability with public switched telephone networks, interoperability with PBXs, etc. Procuring this additional network equipment and testing voice service comes at a cost. User devices best suited to support of voice applications (e.g., PDAs) need to be available for successful deployment of these applications. All of these factors need to be considered when developing a network evolution plan. Due to budgetary constraints, it may be beneficial to phase in these services over time to reduce overall risk.

Some applications may require access to LTE network features that provide the scalability needed for public safety incident response, planned events and day-to-day operations. Delivery of video streams, for example, can require bandwidths in excess of 500 kbps. Public Safety operations may require multiple users on the scene of an incident to view the same video stream simultaneously. Sending each user its own copy of the video stream could consume all the bandwidth available in a sector. To address such scalability issues, LTE supports a feature known as evolved Multimedia Broadcast Multicast Services (eMBMS). eMBMS allows one copy of an IP packet stream to be received by multiple users in the same sector, conserving air interface resources and providing the scalability needed for video multicast and LMR-like voice applications. As will be discussed later, eMBMS functionality is supported by later versions of the LTE standard. As such, support of eMBMS will be part of a public safety network evolution plan.

In the following, we address some of the issues relevant to network evolution in the context of the list of public safety applications described by NPSTC's Broadband Task Force. In general, a measured and progressive approach is recommended for application adoption. The network must first achieve, in general, mission critical operational capability in the realms of performance and capacity, coverage, resilience, and traffic prioritization (refer to 6 Evolution Framework for additional details). Specific applications can then be introduced incrementally, starting with less demanding over-the-top applications and culminating at some point in the future with the most critical and fundamental applications such as LMR voice communication. Applications, including voice, will compete with one another for available bandwidth. As a result, policies and practices along with the relevant supporting technologies will have to be developed based upon incremental knowledge accrued from field experience.

5.1 Over the Top Applications

A number of the applications specified by the NPSTC Broadband Task Force shown below can be supported with best-effort IP data access – a service that will be available on all initial and subsequent LTE network deployments. In the commercial world, such applications are known as "Over the Top Applications" referring to their ability to run on top of a best-effort IP data service without requiring additional integration effort[9]. Data applications currently used by public safety agencies which run over commercial service provider networks, for example, operate as "Over the Top Applications." These applications can be readily migrated to the public safety wireless broadband network, leveraging

[9] Additional integration effort is required for applications to take advantage of special features provided by a network. Such features include, for example, requesting different quality of service treatment for different data streams, access to network-provided geolocation services, and prioritization. In order for an application to use these features, signaling messages must be exchanged with the network.

existing applications, procedures, processes and expertise. All Over the Top Applications can be further enhanced through the use of priority services, services that require the exchange of signaling messages between the LTE network and application to allow the application to request a specific priority treatment.

The use of over the top applications will have an impact on network capacity requirements and perhaps other aspects of the LTE network evolves. Enhanced support for over the top applications through the introduction of priority services or other supplemental security services that are required by public safety must be considered as part of the network evolution plan.

5.1.1 Internet Access

As described in NPSTC's Broadband Task Force report: "Public safety subscribers shall have access to the global Internet. Users will use the Internet both as a way to access home network systems and to access other systems and services available over the public Internet, including but not limited to messaging systems and web servers." The NPSTC Broadband Task Force report recommends that support of internet access be required on all LTE networks deployed on waiver. Even this most basic of all services has specific implications for public safety. For example, consider security and the need to be able to isolate the public safety network from the general internet in certain Cyber-crisis situations. In addition, different jurisdictions control and manage Internet access in different ways: some cities/regions limit Internet access for Emergency Response Providers in the field and/or require policy controls.

5.1.2 VPN Access to any Authorized Site and to Home Networks

As described in NPSTC's Broadband Task Force Report: "The regional operator and commercial networks operating in conjunction with the [Public Safety Broadband Licensee] shall be required to allow establishment and use of VPN connections by roaming users on their networks to other networks." The NPSTC Broadband Task Force report recommends that support of this service be required on all LTE networks deployed on waiver.

5.1.3 Status/Information "Homepage"

As described in NPSTC's Broadband Task Force Report: "Public safety or public/private partnership network operators shall provide a universal method to obtain a "home page" for visitors to the system. This "home page" will facilitate access to and distribution of available applications, alerts, incident-specific information, system status information, and information that the operator deems important to share with visitors to the system." The NPSTC Broadband Task Force report recommends that support of this service be required on all LTE networks deployed on waiver.

5.1.4 Field-Based Server Applications

As described in NPSTC's Broadband Task Force Report: "The regional systems shall support the use of field-deployed server applications. This requirement includes the need for client devices to consistently and continuously reach these server-based systems from any other location on the Internet. The capability is not required for every subscriber device on the broadband network but is limited to a subset of the users that actually require such a feature." Field-based server applications include, for example, Computer-aided Dispatch (CAD) and Records Management Systems (RMS). The NPSTC Broadband Task Force report recommends that support of this service be required on all LTE networks deployed on waiver.

5.1.5 Access to Responders under Incident Command System (ICS)

As described in NPSTC's Broadband Task Force Report: "First responders, emergency response support, and all other mutual aid responders managed under the ICS structure of a requesting agency served by a public safety wireless broadband network shall be provided access to that network to carry out incident objectives and communicate with their home networks." The NPSTC Broadband Task Force report recommends that support of this service be required on all LTE networks deployed on waiver.

5.2 Other Applications

The remaining applications specified by the NPSTC Broadband Task Force require access to LTE network features that will likely not be available in initial LTE deployments, and hence will be factors in network evolution planning. These applications require access to quality of service features, network services (e.g., network assisted geo-location, evolved Multimedia Broadband Multicast Service), or additional services (PSTN voice, SMS-MMS messaging) that require additional equipment that may not be part of an initial LTE network deployment. If additional capabilities have to be deployed a later time in support of these applications, then this will need to be part of a network evolution plan.

5.2.1 Status/Information "SMS-MMS Messaging"

As described in NPSTC's Broadband Task Force Report: "Public safety, public/private partnership, and commercial network operators shall provide the ability for users to send and receive Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages." The NPSTC Broadband Task Force report recommends that support of this service be required on all LTE networks deployed on waiver.

Comment: Many commercial wireless service providers have adopted LTE's IP Multimedia Subsystem (IMS) to support short message and multimedia message services. Deploying IMS is an additional cost. If SMS-MMS Messaging is supported, it will need to be part of the public safety network evolution plan.

5.2.2 Land Mobile Radio Gateway

As described in NPSTC's Broadband Task Force Report: "Networks shall allow for connection and operation of IP-based voice interoperability gateways." The NPSTC Broadband Task Force report recommends that support of this service be required on all LTE networks deployed on waiver.

Comment: Voice packets and signaling messages for this application have stringent quality of service requirements. As a result, access to LMR Gateway Devices from LTE terminals will require support of quality of service in the LTE network. In addition, to provide scalable access to LMR Gateway Devices, downlink transmission (packets sent from the LTE network to LTE devices) may need to be carried over LTE evolved Multimedia Broadcast Multicast Service (eMBMS). eMBMS will not be supported on initial commercial or public safety LTE network deployments. To ensure nationwide interoperability, support of access to LMR Gateway Devices from LTE devices should be based on open standards. These standards have yet to be developed. Because of all these factors, if LMR Gateway Devices are supported, this service will be part of the public safety network evolution plan.

5.2.3 Location Based Data Capability

As described in NPSTC's Broadband Task Force Report: "Regional networks should include the capability to collect and convey subscriber unit location data in real time. The technical ability to convey location information should be inherent on any public safety network and associated commercial networks. Location data should be accessible to appropriate applications, as may be authorized by management level policy. Location data applications may be located on both subscriber units and associated agency level command/control applications. Subscriber units of future public safety networks should meet the same minimum location data information requirements (format and accuracy) as is currently applicable on current commercial services networks in order to retain a broad level of compatibility with incumbent systems." The NPSTC Broadband Task Force report recommends that support of this service is desired, but not required, on all LTE networks deployed on waiver.

Comment: Location fixes can be supported in one of two ways: by reading position fixes from GPS receivers embedded in LTE devices (an over the top application), or by reading position fixes by accessing LTE's geolocation service. LTE's geolocation service has a number of benefits over an over-the-top geolocation application, including the ability to determine a mobile's position when a GPS receiver is unable to resolve a position fix. (This often happens, for example, in dense urban environments where tall buildings can obstruct line-of-site reception with GPS satellites and inside buildings or underground structures, where building penetration losses degrade GPS reception.) If this feature is supported, it will need to be part of an evolution plan.

5.2.4 One-to-Many Communications across All Media

As described in NPSTC's Broadband Task Force Report: "Regional networks should provide one-to-many communications capabilities to outside network users responding in mutual aid to that Regional Network. These communications capabilities should extend from voice, as commonly used in traditional land mobile radio systems, to text messaging, to video, and other forms of data communications. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement." The NPSTC Broadband Task Force report recommends that support of this service is desired, but not required, on all LTE networks deployed on waiver.

Comment: Support of real time voice and video distribution requires quality of service. Scalable delivery of voice or video streams requires the deployment of LTE's evolved Multimedia Broadcast Multicast Service. As eMBMS Service is not yet available, One-to-Many Communications across All Media will be part of the public safety network evolution plan.

5.2.5 Public Switched Telephone Network Voice

As described in NPSTC's Broadband Task Force Report: "Public safety 700 MHz voice capable devices such as cell phones, PDAs, or their equivalent shall be capable of placing and receiving full-duplex telephone calls to any telephonic device on the Public Switched Telephone Network (PSTN) in the visited network with the same functionality that cellular telephones operate nationally today. This includes location based PSAP call routing, E911 Phase II location transmission, and, if necessary CALEA. In the case where the user transitions in to or out of one regional system, the voice session shall be handed off between the two networks with limited loss of audio during the transition. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement."

Comment: Support of PSTN Voice requires support of quality of service and deployment of additional equipment for call handling, interoperability with Public Switched Telephone Networks, and PBXs. Commercial wireless service providers have adopted LTE's IP Multi-Media Subsystem to support PSTN Voice services of LTE and provide interoperability with voice services supported over other commercial wireless technologies. If PSTN Voice will be supported on the public safety wireless broadband network, it will be part of the public safety network evolution plan.

5.2.6 Land Mobile Radio Voice

As described in NPSTC's Broadband Task Force Report: "Networks that provide voice service as an application should provide voice interoperability interfaces to existing agency LMR systems in the area served by the broadband network. Public Safety users on such home or visited networks should be able to call or hail an authoritative dispatch agency or control point using the broadband network subscriber device with microphone and speaker for two-way audio and talk or be connected to other serving agency voice communications resources. Because the devices and device capabilities for this feature will develop over time, this feature may be considered a future requirement." The NPSTC Broadband Task Force report recommends that support of this service is desired, but not required, on all LTE networks deployed on waiver.

Comment: Support of LMR-like voice service over an LTE network will require support of quality of service, LTE's evolved Multimedia Broadcast Multicast Service and other features. Dual-mode devices supporting both an LTE interface and an LMR interface will be required, with the LMR interface providing talkaround service and direct access to P25 networks when LTE coverage is not available. To ensure nationwide interoperability, open standards must be developed to support LMR voice service over LTE. Because of all these factors, if support of LMR Voice is to be supported, it will be part of the public safety network evolution plan.

5.3 Evolution of LTE

LTE standards are developed by the standards body known as 3GPP[10]. Evolution of LTE standards, driven by the needs of the commercial wireless market, proceeds incrementally over a series of *releases*. Each release of the LTE standard provides a new set of features as required by the market,

[10] See www.3gpp.org for additional details.

and a consistent set of specifications from which implementers can build products. New releases of the standards are developed to maintain backward compatibility: LTE user devices built to earlier releases will continue to operate on networks supporting later releases of the standard but may not have the ability to leverage any of the new releases functionality.

Development of the specifications that comprise each release occurs incrementally over three distinct stages, allowing different releases to be developed in parallel:

- Stage 1 specifications define the service requirements from the user point of view.
- Stage 2 specifications define an architecture to support the service requirements.
- Stage 3 specifications define an implementation of the architecture by specifying protocols in details. In addition, specifications related to the testing of each feature are developed in stage 3.

Figure 1, "LTE Standard Releases," gives a high level summary of the two LTE standards releases that have currently been developed (Release 8 and Release 9) and the release currently being finalized by 3GPP (Release 10)

The initial release of LTE is part of 3GPP Release 8. The primary market driver for LTE Release 8 was introduction of IP high speed data. As a result, 3GPP Release 8 provides the features needed to support high speed data transmission, as well as features to support handovers to legacy wireless networks.

The primary market driver for Release 9 was simultaneous support of voice, video and data on an LTE network. LTE voice services defined in Release 9 have full feature parity with the voice services supported over 3rd generation wireless networks, including support of E-911 service.

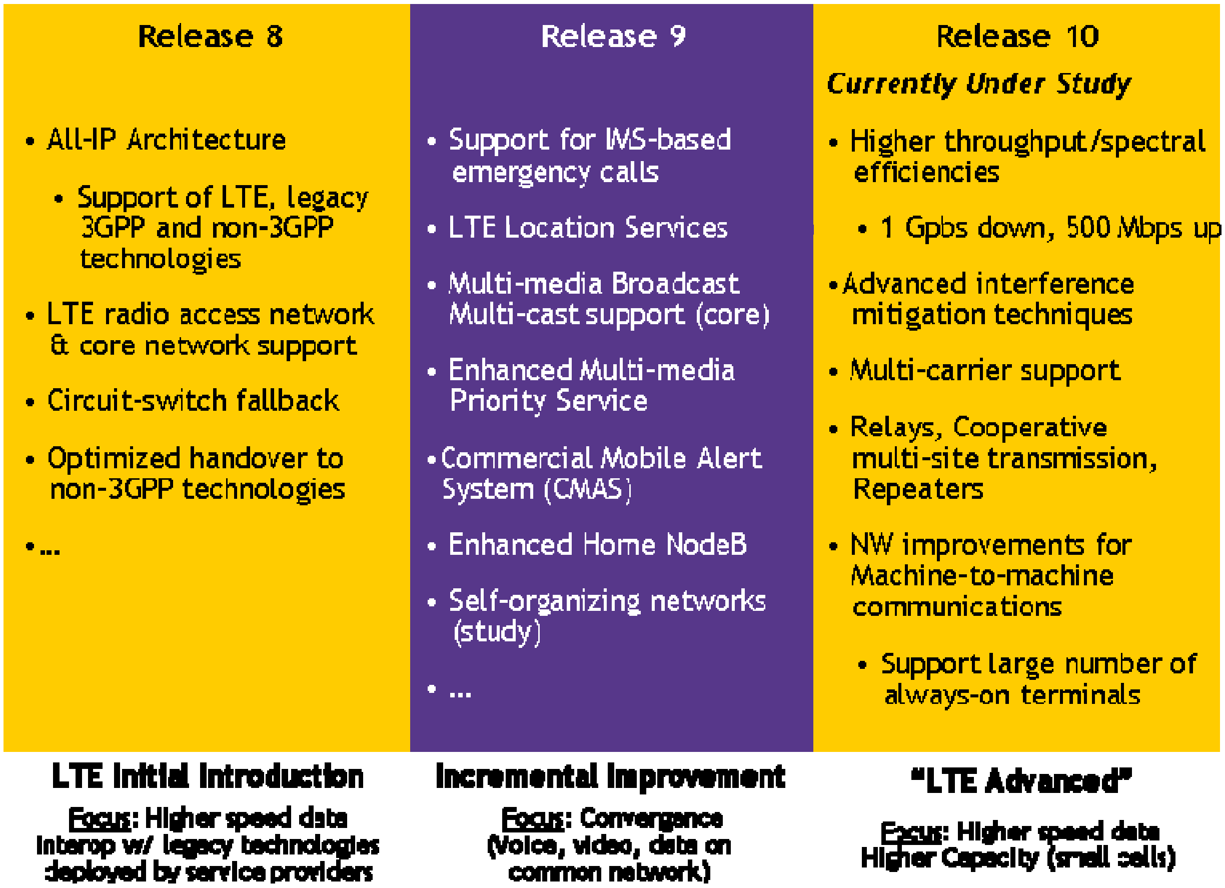
The primary market drivers for the development of the Release 10 standards are increased data rates/spectral efficiencies, coverage improvements (through, for example, the use of relays and multi-site repeaters), support of small cells, support of non-contiguous spectrum blocks (known as multi-carrier support) and support of machine-to-machine communications.

The standardization process ensures development of a consistent set of specifications from which implementers can build products. Completion of a standards release, however, does not necessarily guarantee implementers will build products supporting all the features appearing in the release.

Implementing a feature involves companies across the LTE ecosystem: service providers, chipset manufacturers, user device manufacturers, network infrastructure manufacturers, software developers, etc. Market needs that were anticipated when planning for a release first began may have changed by the time implementation negotiations begin. As a result, a subset of the features in each release typically initially gets implemented. Additional features may be phased in at a later stage or may never be developed.

This dynamic has important implications for planning the evolution of the public safety LTE network. Each LTE release provides additional functionality that will be beneficial to public safety. Public safety evolution plans must take into account both the features planned for each LTE release and what actually gets implemented (and when). Specific features required by public safety may not be supported by

LTE. In these cases, either alternative ways must be found to realize the desired functionality or new functionality introduced into the 3GPP standards.



Release 8

- All-IP Architecture
  - Support of LTE, legacy 3GPP and non-3GPP technologies
- LTE radio access network & core network support
- Circuit-switch fallback
- Optimized handover to non-3GPP technologies
- …

LTE Initial Introduction

Focus: Higher speed data
Interop w/ legacy technologies deployed by service providers

Release 9

- Support for IMS-based emergency calls
- LTE Location Services
- Multi-media Broadcast Multi-cast support (core)
- Enhanced Multi-media Priority Service
- Commercial Mobile Alert System (CMAS)
- Enhanced Home NodeB
- Self-organizing networks (study)
- …

Incremental Improvement

Focus: Convergence
(Voice, video, data on common network)

Release 10

Currently Under Study

- Higher throughput/spectral efficiencies
  - 1 Gpbs down, 500 Mbps up
- Advanced interference mitigation techniques
- Multi-carrier support
- Relays, Cooperative multi-site transmission, Repeaters
- NW improvements for Machine-to-machine communications
  - Support large number of always-on terminals

"LTE Advanced"

Focus: Higher speed data
Higher Capacity (small cells)

Figure 1. LTE Standard Releases.

6 Evolution Framework

This section outlines the major considerations that must be taken into account in planning the evolution of the network.

6.1 Commercial Technology

There is an intrinsic tradeoff between capability/currency and stability/predictability in the adoption of new technology (a risk vs. reward tradeoff). On one hand, staying current with commercial technology provides economies of scale, interoperability and affords public safety with best-in-class technology. On the other hand, the standard of reliability and predictability for technology that is used in mission critical situations must be absolutely predictable and reliable. Since the public safety wireless broadband network will employ a commercial technology (LTE), it is important for the network to keep pace with industry advances but in a measured manner. To maximize the stability of the technology, the timing of rollout of each increment (e.g., 3GPP Releases) of technology should lag that of the commercial markets, allowing public safety to take advantage of the vast amount of testing performed by commercial carriers. While this may be prudent in order to ensure adequate technology maturity, it may also be dictated by sheer logistics. The challenge here could be to ensure that funding sources are sufficient to keep up with the pace of commercial technology adoption (albeit somewhat phase shifted to allow for maturation).

- The 3GPP specification process for LTE ensures backward compatibility from one LTE release to the next.
- 3GPP specifications do not require instantaneous synchronization of LTE releases across different networks.

Not all portions of the standard are being implemented by vendors and the commercial network operators; furthermore, not all operators are implementing the standards in exactly the same ways (e.g., some optional features maybe selected by one carrier and not another). Introduction of many capabilities require complex coordination across networks and devices. For example, eMBMS requires changes to the infrastructure (eUTRAN and Evolved Packet Core) as well as to device chipsets and software. Taking advantage of this new network functionality may require network software upgrades, deployment of new network equipment, and replacement or reprogramming of user devices[11].

- Public safety should review the specification in conjunction with vendors and network operators to determine a feature/function set which best suits public safety.
- Once a governance group is put into place, regulators should not mandate any of the LTE standards as network requirements; rather, this should be left to the standards bodies and the public safety wireless broadband governance group. The public safety wireless broadband governance group should, in contemplating network evolution, consider early (waiver) deployments and accommodate them into the evolution of the nationwide network.
- Regulators should review any proposed rules and requirements with the public safety wireless broadband governance group and secure this group's approval before the rules and requirements are enacted.

6.2 Compatibility

As commercial technology evolves, new capabilities are introduced. Public safety will need to determine what new capabilities it would leverage for its applications, plan an introduction roadmap, and also ensure that uses of earlier technology is not compromised. This primarily affects four aspects:

- Application to Application: This involves ensuring that devices/clients are compatible with other corresponding devices/clients (peer to peer) as well as between the device/client and the network components of the application (e.g., device client to application server such as a database).

[11] As a result, public safety user devices will likely have a much shorter useable life compared to Land Mobile Radio user devices.

- Device to Network: This is the area of most scale and individual impact. The evolution plans must consider the useful life / support window for devices on the network and plan the introduction of new technology to accommodate this compatibility window.

- Network Element to Network Element: This comes into play as new capabilities are introduced into the network and the updates involve more than one entity in the network and implicitly impact the interfaces between network elements. Introduction of new capabilities (software or hardware) may need to be coordinated to ensure that all impacted elements are properly orchestrated and supported.

- Network to Network: There are four main areas of consideration for this.

    - Regional deployment to regional deployment (roaming considerations, network sharing arrangements)

    - Public Safety network to carrier network (primarily roaming considerations)

    - Public safety wireless broadband Network to Public safety P25/LMR Network

    - Public safety wireless broadband Network to Satellite (to the extent that Satellite networks are leverages as part of the coverage approach).

6.3 Coverage

As the network is built out, it is expected that it will incrementally expand to increase geographic coverage. As regional networks “grow” together, it will be important for the evolution to take into account a cohesive RF plan and interconnect strategy (e.g., as rural areas add RF coverage, they could be hosted by urban or state-wide core networks). Other technologies, such as satellite communications, can provide network restoration or extend networks into key areas where terrestrial networks are insufficiently built out or where existing networks are disrupted or destroyed. Successful deployment of alternative technologies often requires that attention be paid to pre-positioning and training with the equipment in question.

Coverage is more complex to engineer in LTE broadband networks since it has many variable components. In general, uplink and downlink user throughputs diminish as one moves from cell center to cell edge (by potentially an order of magnitude or more). User data rates (and, hence, overall capacity) are also affected by adjacent cell activity (interference). This is much different than today’s LMR systems, for example. As application types (and priorities) vie for this dynamically varying bandwidth,, the network will have to adapt in real time to ensure that the highest priority applications and users are served in the best way possible.

6.4 Capacity

As usage of the network increases, capacity may need to be enhanced. Capacity enhancements will affect RF planning as well as the increase the signaling and bearer traffic loads on core networks. Addition of capacity is typically accomplished through the addition of cells (the initial network may be built on a relatively sparse grid) or the purchase of satellite capacity for restoration capabilities. As more traffic flows through the core networks (more traffic on existing sites and more sites in total), the core networks may need additional capacity. Capacity engineering guidelines may be defined and published relative to support for classes of public safety applications and the number of concurrent instances of an application class that can be supported by a given data rate. These would be input to network engineering activities and would help align expectations of network performance overall; however, it is unrealistic to mandate minimum supported rates/performance unilaterally across all networks and locations within the networks. Capacity planning must be coordinated between regional portions of the network and shared national components to ensure that the entire network scales end-to-end. NOTE: These decisions (RF and Core) may be left to regional/local network operation as well.

6.5 Resiliency

As the network topologically evolves (sites are added, cores are added, etc.), overall consideration of network resiliency has to be continually evaluated. This is necessary to ensure that application centers, cores (EPC), interconnect/backhaul, and RF (where applicable) redundancy is properly engineered and maintained to the necessary standards. Resiliency has to be applied at the regional level to ensure that each such deployment is robust but also must be applied on a national scale for network assets that are truly operated nationwide (e.g., an IP backbone used to interconnection regional deployments). This involves ensuring adequate equipment redundancy to serve expected capacity, geographic redundancy to protect against localized disasters, etc. To maximize resiliency, the availability and use of multiple communications technologies and RF bands should be considered.

6.6 Security

As new security threats come into being and additional/improved methods to secure information are devised, it will be useful to employ nationwide coordination of best practices and real time response to threats. Further, in many cases, security changes must be coordinated if users across the nation are to still have access in an interoperable manner. The nationwide governance structure must include support for a center for security and cybersecurity best practices and standards.

7 Conclusions

An important element of the FCC’s policies surrounding development of a nationwide public safety wireless broadband network is establishment of a network evolution framework that will enable public safety officials to leverage the technological advancements that regularly occur in the wireless industry. In doing so, the FCC provides greater assurance that Emergency Response Providers will have access to the most advanced communications capabilities possible and that the nationwide public safety wireless broadband network will keep pace with innovations occurring in the private sector.

Successful network evolution necessitates striking a suitable balance between the risks, benefits and costs of adopting or not adopting new technologies as technologies and mission requirements evolve. Toward this end, the Network Evolution Working Group has developed and presented a series of recommendations to help ensure the United States’ Emergency Response Providers are able to effectively, and in a cost efficient manner, take advantage of new technologies in a way that best supports public safety mission requirements and sustains nationwide interoperability.

8 References

[1] "NPSTC 700 MHz Public safety wireless broadband Task Force Report and Recommendations," September 4, 2009. (http://www.npstc.org/documents/700_MHz_BBTF_Final_Report_0090904_v1_1.pdf)

[2] "National Forum on Public safety wireless broadband Needs," August 23, 2010. (http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf)

9 List of Acronyms

3G	3rd Generation
3GPP	3rd Generation Partnership Project
CAD	Computer-aided Dispatch
CALEA	Communications Assistance for Law Enforcement Act
CMAS	Commercial Mobile Alert System
COPS	Community Oriented Policing Services
E911	Enhanced 911
eMBMS	evolved Multimedia Broadcast Multicast Service
EPC	Evolved Packet Core
ERIC	Emergency Response Interoperability Center
eUTRAN	evolved UMTS Terrestrial Access Network
FCC	Federal Communications Commission
Gbps	Gigabits per second
GPS	Global Positioning System
ICS	Incident Command System
IMS	IP Multimedia Subsystem
IP	Internet Protocol
kbps	kilobits per second

LMR	Land Mobile Radio
LTE	Long Term Evolution
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input Multiple Output
MMS	Multimedia Messaging Service
NPSTC	National Public Safety Telecommunications Council
OFDMA	Orthogonal Frequency Division Multiple Access
P25	Project 25
PDA	Personal Digital Assistant
PSAC	Public Safety Advisory Committee
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RF	Radio Frequency
RMS	Records Management System
SMS	Short Message Service
UASI	Urban Areas Security Initiative
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network