TOWARD A NEXT GENERATION NETWORK FOR PUBLIC SAFETY COMMUNICATIONS

Dale N. Hatfield and Philip J. Weiser

Silicon Flatirons Program
University of Colorado School of Law

May 17, 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The University of Colorado Law School's Silicon Flatirons Program Roundtable on Public Safety Communications (herein, the "Roundtable") emphasized that a progressive view of public safety communications must be a central feature of sound homeland security policy going forward. Over a two day period (April 11-12, 2007) in Washington, D.C., Roundtable participants—with affiliations spanning a variety of disparate stakeholders—tackled the increasingly high-profile and often acrimonious issues surrounding the state of United States public safety communications. Rather than evincing entrenched and inflexible views, however, discussants deftly identified shared priorities, addressed next generation technological solutions, and provided thoughtful analysis toward finding solutions which will address challenges facing public safety in the near and long term. This Silicon Flatirons Report (the "Report") attempts to capture the spirit and high quality of the Roundtable's discussion. As more fully explained in the Report, several noteworthy points emerged from the Roundtable, including the following:

The migration to next generation networks represents a crucial opportunity to introduce a new paradigm whereby public safety is conceived of as an enterprise. Going forward, public safety agencies must adopt a broader view of communications technology, embracing the idea of a converged ecosystem. Over time, they will need to transition away from specialized networks built solely for and operated solely by public safety agencies. Notably, because the public safety enterprise spans geographic jurisdictions, encompasses different agencies, and cuts across local, state and federal governmental spheres, it is crucial that all parts of a next generation public safety communications system be developed in concert so that tomorrow's overall network (which will, by necessity, incorporate different networks, (i.e., resemble a "network of networks")) is greater than the sum of its parts. Stated simply, individual public safety agencies will achieve greater communications capabilities if they are willing and able to work together and rely on communications technology that they may not exclusively own or control. Note that this does not mean that one size must fit all: it is imperative that tomorrow's network accommodate tailoring to localized needs; however, such tailoring should be achieved within a larger interoperable and coordinated communications system. To facilitate interoperability and achieve economies of scale, networks should be operated at higher levels and local agencies should be empowered with the ability to use information and communications technology as needed without bearing the responsibility for running advanced networks.

The development of a next generation network ("NGN") for public safety presents an inflection point for today's first responders: such networks should be broadband, Internet Protocol (IP)-based and capable of handling voice, data, image, video, and multi-media content. The current public safety system, taken as a whole, is compromised by fragmented systems using disparate bands of spectrum and incompatible standards which cause both operability and interoperability problems. The piecemeal development of incompatible systems was not irrational: it largely occurred in a prior technological age in which today's seamless wireless capabilities were barely fathomed. Nonetheless, in order to properly equip the nation's first responders, communications systems must leverage twenty-first century technologies. Significantly, today's narrowband channels and other aspects of current public safety architecture essentially preclude existing systems from evolving into next generation broadband networks capable of seamlessly handling voice, data, image and video traffic on a common platform (i.e., the type of transformation that is already well underway in commercial cellular radio systems). To be sure, today's interim solutions—such as the Project 25 (P25) standard and use of gateways—help bridge interoperability deficiencies and diminish operability shortcomings. They suffer, however, from notable drawbacks and are not long term solutions. For example, the P25

standard's narrowband technology is not a path to supporting broadband applications and is limited in its ability to leverage commercial broadband developments. Additionally, gateway or network-based solutions, while helpful in resolving near-term interoperability problems, are hindered by drawbacks such as spectrum inefficiency and are not an ideal (or effective) long term solution. In short, public safety organizations have identified a pressing need for broadband capabilities and policymakers are just beginning to develop strategies to facilitate this development.

General principles to guide the development of an NGN for public safety include reliability, security, openness, modularity, extensibility, and reliance on commercial, broadly supported standards. An NGN for public safety should benefit from the economies of scale and scope (i.e., the larger competitive ecosystem) associated with commercial systems while meeting the continuing public safety community needs for mission critical voice communications. Notably, it is critical that an NGN be attentive to the specialized needs of the public safety community. Thus, the requirements for public safety's mission critical voice capabilities must be included in the initial specifications for a public safety NGN so as to develop systems that will eventually be capable of handling all traffic on a fully converged network which captures economies of scope, improves spectrum efficiency, and reduces the need for gateways. These needs include rapid call setup time and group calling capabilities which are representative of modern narrowband public safety systems, as well the other features including multiple talk-groups, talk-around capabilities, multi-level priority access, preemption and end-to-end encryption for privacy and security.

As public safety moves toward an NGN featuring higher level network operation, NGN coordination models should be carefully considered and fleshed out. A public safety NGN will increasingly migrate away from the old regime of isolated actors making autonomous communications decisions and, instead, public safety will transition to a paradigm of inter-agency and cross-jurisdictional network coordination. Against this backdrop, two dominant NGN models have emerged: the "government as contractor" and the "public safety spectrum licensee." Under a government as contractor model, government entities contract out for the development of a next generation network. Recent case studies in New York City and the Washington, D.C. area's National Capital Region Interoperability Program provide real world examples of such a model. Under this approach, if the government defines the terms effectively, then front-end competition creates valuable efficiencies and, moreover, a governmental commitment to a period of years can help entities avoid paying all capital costs up front. Meanwhile, the principal alternative NGN model—a "public safety spectrum licensee"—has garnered attention in connection with the 700 MHz proposal now being floated by the FCC. This model generally involves the use of a non-profit body that possesses a license to spectrum and oversees the use of that spectrum, which may well be shared with other commercial users. The most critical question related to the public safety licensee model is how the relevant governance structure would work in practice: it is important that the licensee be well positioned to ensure that the cooperating private firm meets its commitments and, consequently, an effective enforcement mechanism is particularly important.

In many respects, the near term presents the most challenging public safety funding demands of all—policymakers must both make do with legacy systems and facilitate the development of an NGN system. The transition to an NGN will not happen overnight. Given public sector funding cycles and constraints, existing public safety narrowband systems will remain in place for many years to come and hence backward compatibility of any NGN will remain critical to assure interoperability. Ultimately, once a next generation system is well proven and adopted by public safety agencies, there may well be an opportunity for those

agencies to abandon their legacy equipment and, in some cases, traditional spectrum allocations. But such a day is both far off in the future and uncertain. In the meantime, policymakers face the dual challenges of facilitating the development of the best possible technologies to work in conjunction with existing systems, as well as laying the groundwork for a next generation architecture.

During the transition to a public safety NGN, perfection should not be the enemy of the good. Progress toward an NGN must be cognizant that it is impractical to build a network with sufficient capacity to handle all communications needs—essential as well as non-essential—in times of emergency. Accordingly, priority schemes and other methods of shedding non-essential traffic will remain critical. Moreover, obtaining the last few percentage points of geographic and in-building coverage becomes prohibitively expensive in any radio-based system designed to cover a wide geographic area and, at some point, cost constraints must be acknowledged. For example, the costs of extending coverage into the third sub-basement of a major bank building may well exceed the public safety benefits. We recognize that such choices are not easy ones—obviously, in cases where coverage or capacity is sacrificed, the ability of public safety agencies to protect the public will be hampered—but they must be made based on reasonable cost-benefit tradeoffs. Thus, the touchstone for an NGN should not be whether such systems are impervious to defect; rather, it should be whether an NGN will deliver significantly improved and cost-effective capabilities to first responders over today's existing networks.

Finally, a critical element of developing a workable NGN for public safety is the development of reasonably effective governance strategies. Given the numerous agencies that need to cooperate with one another as part of an NGN for public safety, no governance system will be perfect and no governance system will enjoy enthusiastic support from all stakeholders. It is clear, however, that the *status quo* and lack of effective cooperation is a recipe for perpetuating today's public safety communications shortcomings. To date, neither the FCC nor the Department of Homeland Security grants have galvanized strategic planning and coordination at the regional or state levels to the degree necessary to transform the autonomous and fragmented culture of public safety communications. In short, different local agencies will have to compromise and give up some control over what communications systems they use, thereby enabling effective coordination with one another. Without such coordination, different agencies could never develop and abide by shared governance rules that will specify how the next generation network will operate (i.e., what services will be available to whom under what circumstances).

For America's public safety agencies, the decision to invest in state-of-the art information and communications technology is long overdue. The first step in doing so, however, is for policymakers to realize that this investment is as critical to the success of these agencies as providing them with effective equipment to protect our citizenry and respond to emergency situations across a range of life-and-death situations. This Report offers a roadmap for how policymakers should evaluate that investment and make it a reality.

PREFACE

This Report emanates from the ideas generated by the University of Colorado Law School's Silicon Flatirons Program Roundtable on Public Safety Communications held in Washington, D.C. on April 11-12, 2007. In this Report, the authors—who moderated the discussion and compiled a relevant set of background readings—endeavored to reflect the spirit of Roundtable discussion. In so doing, participants' analysis and suggestions were distilled into thematic technical and policy strategies for public safety communications. Additionally, to produce a coherent Report, parts of the document necessarily went beyond Roundtable discussion in order to provide additional context and information. Thus, unless specifically attributed, none of the comments, opinions, or ideas in this Report should be taken as embodying the views or carrying the formal endorsement of any specific Roundtable participant.

The authors thank a number of individuals who made this Report possible. For starters, both Mike Altschul and Chris Guttman-McCabe at CTIA—The Wireless Association® deserve credit for recognizing the important opportunity to bring together thought leaders in this area to develop a constructive discussion. In addition, Jon Peha, Professor of Electrical Engineering and Public Policy at Carnegie Mellon University, was an invaluable resource in preparing for the Roundtable, making astute comments during the event, and helping to develop and refine this Report. At Silicon Flatirons, Jill Van Matre worked tirelessly to help put the Roundtable together, research relevant readings, and improve greatly the form and substance of the Report, while Brad Bernthal provided his usual incisive analysis in helping to shape the plans for the event and offering very valuable feedback on the Report itself. Finally, we remain in awe of the level of good will, intellectual engagement, and support for this project shown by all participants through the process. Indeed, that spirit and the constructive engagement that produced this report are a testament to the ability of the communications policy community to come together on such an important issue facing our country.

INTRODUCTION

The University of Colorado Law School's Silicon Flatirons Program hosted a Roundtable on Public Safety Communications on April 11-12, 2007 (herein, the "Roundtable"). This Roundtable was made possible with a generous grant from CTIA—the Wireless Association®—and was held in Washington, D.C. Participants included leaders in the public safety community, wireless service providers, device manufacturers, engineers, and key scholars. A full list of Roundtable participants is attached as Appendix C.

Many of the participants have known each other for years, either as colleagues, competitors, or adversaries in various regulatory battles. With so many different perspectives and stakeholders represented, the potential for conflict among participants was high. Fortunately, the Roundtable proceeded with an impressive level of collegiality and willingness to collaborate. This Report distills the thoughtful analysis and suggestions featured during the Roundtable's discussion into a coherent description of the challenges facing public safety communications and the near and long term solutions for solving them.[1]

Overall, the Roundtable discussion emphasized that technological changes and policy reforms can spur the development of a next generation network that will facilitate interoperability and enable public safety to utilize new technologies that will enhance its effectiveness. All of the participants recognized the importance of addressing both the more immediate need of finding cost-effective solutions to enable interoperability across networks, as well as policies to facilitate the adoption of new, broadband and Internet-based technologies. Similarly, the participants emphasized that the effective resolution of these policy challenges would require the development of a thoughtful strategic vision, political will to invest in public safety's use of information and communications technology, and leadership to implement a new policy direction effectively.

With its Ninth Proposed Rulemaking, the FCC has taken the important step of endorsing the concept of a nationwide interoperable broadband communications network.[2] As we develop the plans for such a system, however, we must have realistic expectations about the time and effort it will take to implement it effectively. Moreover, no system will be perfect, as the real world will demand compromises between the ideal level of coverage and reliability and what is possible given technical and financial constraints. Nonetheless, the current limitations of public safety communications systems—in terms of both operability and interoperability—are a weakness of our national and local emergency response capabilities. This weakness, which is recognized most poignantly in the aftermath of tragedies like that of 9/11 and Hurricane Katrina, is a day-to-day reality for public safety agencies. Until we make progress along a new policy direction, they will continue to use antiquated equipment and be limited by the shortcomings of today's public safety communications.

---

[1] The reader should note that, while this Report aims to reflect the significant contributions and the spirit of the Roundtable's discussion, it is written from the perspective of the authors. Where appropriate, the Report identifies the general sentiment of the Roundtable as a group or the specific view of an individual participant. ***Unless specifically attributed, however, none of the comments or ideas in this Report should be taken as embodying the views or carrying the endorsement of any specific participant at the Roundtable.***

[2] In the Matter of Implementing a Nationwide Broadband Interoperable Public Safety Network in the 700 MHz Band and the Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, *Ninth Notice of Proposed Rule-Making*, 21 F.C.C.R. 14837, PS Docket 06-229, WT Docket 96-86 (Dec. 20, 2006), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-181A1.pdf [hereinafter Ninth NPRM].

This paper proceeds in four major parts. Part I provides technological background, including the evolution of modern public safety communications systems and their attendant technological and operational limitations. Part I also addresses the technological requirements, architecture and possible constraints associated with a next generation network. Part II looks at strategies for implementing a next generation architecture. It begins with a description of legacy regulatory strategies and proceeds to analyze possible policy strategies for a next generation network (along with its associated challenges and opportunities). Part III sets out key concerns for the transition period, including working within the current technological framework, building a sustainable funding base, and establishing clear requirements and standards. Finally, Part IV offers a short conclusion.

PART I: TECHNOLOGICAL BACKGROUND

In order to fully appreciate the technological choices now facing our nation's public safety entities, it is important to understand: **first**, the evolution of public safety communications systems—how we got where we are in terms of modern wireless public safety communications systems; **second**, the technological and operational limitations of such modern public safety systems; **third**, the requirements, architecture and other ingredients associated with an NGN for public safety; **fourth** and finally, the essential considerations that will inform and, in some cases, constrain the development of an NGN designed to meet the needs of public safety in the coming decades.[3]

Accordingly, the balance of this Part I is divided into four sections: Section A, entitled "Evolution of Modern Public Safety Communications Systems," begins by identifying traditional land mobile radio services (i.e., voice dispatch, voice telephony, one-way paging and two-way data communications). It goes on to trace the history of wireless communications systems in public safety applications including the types of systems deployed over time and how, in the quest for additional spectrum, public safety systems came to be deployed in multiple bands in the radio spectrum. It also includes a discussion of the essential features of a modern, voice- and dispatch-oriented, wide coverage area, digital trunked public safety communications, system such as those built around the Project 25 (P25) set of standards.

Section B, entitled "Limitations of Modern Public Safety Systems," provides a high level discussion of how the technological capabilities of such systems are increasingly trailing behind the capabilities of modern commercial mobile radio systems (e.g., in terms of data rates and support of multimedia applications). It also addresses the critical issues of interoperability, spectrum efficiency and the more constrained "ecosystem" associated with specialized public safety networks as compared to the huge economies of scale (and, increasingly, scope) associated with modern commercial mobile radio systems.

Section C, entitled "Requirements and Other Ingredients for a Next Generation Network for Public Safety," provides a high-level view of requirements for an NGN for public safety and postulates a potential architecture based upon a modern, broadband, Internet Protocol (IP) network. It discusses how such a network would benefit from the economies of scale and scope (i.e., the larger competitive ecosystem) associated with commercial systems while meeting the continuing public safety community needs for mission critical voice communications. Notably, such a national network, if deployed, would not instantly become the sole national emergency communications network, but rather would become a critical part of a "network of networks." At least for the foreseeable future, it would need to be interconnected with a broader range of networks that includes not only legacy tactical radio systems, but also public wireless devices and inter-organizational wired voice and data systems (private and commercial) as well.

Finally, Section D, entitled "Essential Considerations in the Development of the Next Generation Public Safety Network," describes some key practical considerations that will impact on the deployment of the NGN. These practical considerations include: (a) the fact that wireless communication by its very nature will always suffer from some gaps in coverage (e.g., in-building) and that "real world" cost constraints prevent radio-based networks of all types from

[3] Portions of Part I are drawn directly from: Dale N. Hatfield, *The Technology Basis for Wireless Communications*, in THE EMERGING WORLD OF WIRELESS COMMUNICATIONS, ANNUAL REVIEW OF THE INSTITUTE FOR INFORMATION STUDIES (Institute for Information Studies 1996).

providing "perfect" coverage; (b) it is impractical to build a network with sufficient capacity to handle all communications needs—essential as well as non-essential—in times of emergency, and hence priority schemes and other methods of shedding non-essential traffic will remain critical; (c) given public sector funding cycles and constraints, existing public safety narrowband systems will remain in place for decades to come and hence backward compatibility of any NGN will remain critical to assure interoperability; and (d) public safety agencies will continue to need to communicate with people and organizations that will never be part of a new NGN.

A. Evolution of Modern Public Safety Communications Systems

(1) Land Mobile Radio Services

Traditionally, the land mobile radio market has been divided into four segments serving four different applications. These applications are one-way paging or messaging (e.g., "beepers"), two-way dispatch, two-way telephone service, and two-way data or text messaging. These applications or services can be provided on a private (self-provisioned) basis, on a "private carrier" or similar basis, or on a common carrier or commercial basis.

Two-way dispatch communications involves communications between and among a dispatcher and units (mobiles and/or portables) in the field. Traditionally, it is a "command and control" system where a high degree of coordination among the units is required. There is typically a requirement for the dispatcher (or a unit in the field) to be able to reach multiple units simultaneously in what is referred to as group or fleet calling (i.e., one-to-many as opposed to one-to-one communications). The voice messages are typically of short-duration (tens of seconds) and require rapid call setup. In its pure form, voice dispatch communication does not involve interconnection with the ordinary public switched telephone network.

Two-way mobile telephone service, in contrast, allows the user to place and receive ordinary voice telephone calls (i.e., one-to-one as opposed to one-to-many communications). The voice messages are typically of longer duration (several minutes as opposed to tens of seconds in the case of dispatch). Because the call itself is of longer duration, and because the person being called is not expected to be instantly available (i.e., the phone must be rung), call setup time is less critical.

Voice dispatch services, sometimes referred to as "walkie-talkie," "push-to-talk/release-to-listen" or simply "push-to-talk" services, are still widely used by many businesses like construction firms, tow-truck operators, and taxicab companies. Additionally, these services remain absolutely essential to police, fire and emergency medical agencies. In the past and up until today, public safety entities have obtained mission-critical narrowband voice dispatch services by operating their own private wireless networks on radio channels that have been allotted by the FCC for public safety use. These allotments were separate from the allotments for services such as mobile telephone, one-way paging or two-way data that were offered on a third-party, "for hire" basis by commercial operators. Increasingly, public safety agencies augment their self-provided, mission-critical voice dispatch service with other services obtained from commercial operators.

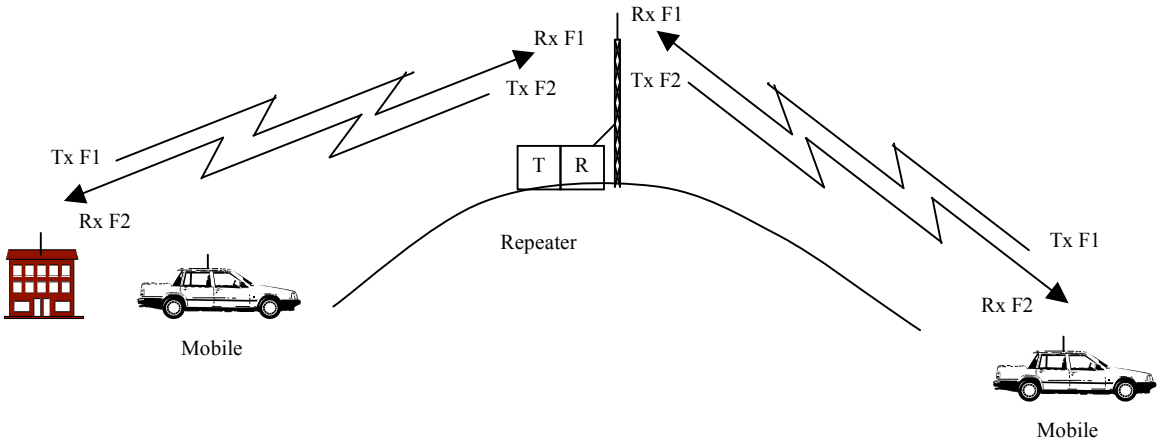
(2) Technological History

One of the earliest uses of land mobile radio was by the Detroit Police Department which began experimenting with a one-way (i.e., base-to-vehicle) system in 1921. These early voice systems used Amplitude Modulation (AM) and were located just above the AM broadcast band in

the Medium Frequency (MF) portion of the radio spectrum. The first license for a mobile transmitter was issued in 1932. A few years thereafter the first Very High Frequency (VHF) band came into use and the much more effective Frequency Modulation (FM) was introduced. Over time, increased use of land mobile radio by public and private entities led to the opening of another band higher in the VHF region. These two mobile radio bands in the 40 MHz and 150 MHz portion of the VHF range became known as Low Band and High Band respectively. These early voice systems operating at both Low Band and High Band basically consisted of a base station transmitter-receiver combination, an antenna tower and antenna, and the individual mobile transmitter-receiver units (transceivers). These early systems operated in the push-to-talk, release to listen mode and provided voice dispatch services using a single frequency for both transmitting and receiving. Because of an overall scarcity of frequencies, these channels were often shared with other jurisdictions.

With the continuing growth in the land mobile radio services, the FCC eventually allotted additional spectrum for public safety and other groups in the Ultra-High Frequency (UHF) portion of the radio spectrum. In allotting additional spectrum in the UHF region (450 MHz – 470 MHz), the FCC set aside two frequencies for each channel of communications—one to transmit and one to receive. Providing a pair of frequencies instead of one creates several advantages, including reducing the interference between higher power base stations and typically much lower power mobile units. Most significantly from a public safety perspective, it allowed for the introduction of repeaters which can provide greatly increased geographic coverage, especially for mobile-to-mobile and portable-to-portable communications. The repeater is typically installed on a very high tower, building or mountaintop. As illustrated in Figure 1, a repeater receives a low power mobile, portable or base station signal on one frequency and retransmits it at high power on the second frequency of the pair. Because of its advantageous location, the repeater can normally receive and transmit over a wide area. This means that two low power mobile or portable units that are unable to communicate directly even though they are only a few miles apart can successfully communicate via the repeater because they are both within its line-of-sight. This arrangement facilitates the rapid voice call setup and group calling among and between a dispatcher and field units that is the *sine qua non* of public safety voice communications.

FIGURE 1: CONVENTIONAL REPEATER SYSTEM



Conventional public safety systems of the type set out above can provide access to more than one channel but channel selection is done manually by the dispatcher and units in the field.

This is in contrast to the multi-channel trunked systems described below where channel selection is done automatically under the control of computer logic.

Rapid growth in the use of conventional dispatch systems described above continued and in the late 1960s the FCC once again began to consider the reallocation of additional spectrum for public safety land mobile radio systems—this time in the 800 MHz region of the radio spectrum. In doing so, the agency wanted to encourage the development and deployment of systems that utilized the increasingly scarce radio spectrum on a more efficient basis. One attractive way of improving spectrum efficiency is through the use of trunking. Without trunking, each dispatcher (base) or mobile unit operates on a single channel that may be shared with other licensees. Thus, a dispatcher or mobile unit desiring to make a call cannot do so if that single channel is busy. Moreover, the dispatcher or mobile unit cannot complete the call (i.e., it is blocked or queued) even though it is very likely that other single channels in the geographic area may be unused at that moment. Finally, users of an untrunked (i.e., conventional) single channel cannot make that channel available to users on other channels even if it is not being used.

By contrast to conventional systems, the individual channels in a trunked system are placed into a pool and made available to different groups of users on an on-demand basis. More specifically, a dispatcher or mobile unit desiring to make a call is given a channel to use for the duration of the call (or transmission) and, at the end of the call or transmission, the channel is returned to the pool for use by other users. Note that with trunking, a call or transmission can be completed if any of the channels in the pool are idle and, conversely, a call is not blocked or queued unless all channels in the pool are busy.

Systems employing trunking are known as multi-channel trunked system and one popular form utilizes what is known as centralized trunking. With centralized trunking, status information (i.e., busy or idle) on each channel in the pool is maintained in a central controller and one channel from the pool is designated as a control channel. Idle dispatcher and mobile units monitor the control channel. If a unit initiates a call (i.e., by pushing the push-to-talk button), the calling unit sends a signaling message on the control channel to the central controller identifying the called group and requesting a channel from the pool. The central controller identifies an idle channel and responds on the control channel with a signaling message that instructs the calling and called units to tune to the selected idle channel. Units that are not a member of the called group continue to monitor the control channel. The conversation can begin when the calling and called units arrive on the selected channel—i.e., once the call has been set up. In a modern multi-channel trunked system, this whole process (i.e., the call setup time) takes place in less than one-half second.

Trunking can provide dramatic improvements in spectrum efficiency and/or performance (in terms of fewer blocked or delayed calls) and, as explained in more detail below, offers important other advantages as well. Thus, in 1975, when the FCC allocated additional spectrum for private land mobile radio (including public safety) in the 800 MHz band, it authorized not only conventional, single channel dispatch systems, but multi-channel trunked systems as well.

The use of sophisticated signaling and computer logic in the centralized controller of a modern multi-channel trunked system facilitates the inclusion of advanced features that are particularly important in public safety applications. If the traffic load is very heavy due to emergency conditions, for example, higher priority calls can be moved to the head of the queue and given the next channel that becomes available. Or, in the alternative, an existing lower priority call can be preempted by a higher priority (e.g., “officer down”) call. Perhaps most important in terms of this Report, a multi-channel trunked system can provide effective

interoperability among all dispatch and mobile units sharing the system. For example, if two jurisdictions have separate, conventional, single-channel systems, they may not be able to communicate with one another in times of emergency or they may only be able to do so by employing gateways (e.g., cross-band repeaters) that require difficult coordination and/or are inefficient in terms of their use of the radio spectrum. In a multi-channel trunked system, each of the two jurisdictions would have its own separate talk-group or a "virtual network" that is defined in the software residing in the central controller. In times of emergency, units in the two jurisdictions can join pre-formed talk-groups or virtual networks that allow efficient communications between and among the units in both jurisdictions. Of course, such opportunities require ongoing cooperation (e.g., multi-agency agreements), such as that necessary to maintain shared access to different databases.[4]

The public safety community took advantage of the opportunity to deploy modern multi-channel trunked systems that met their requirements for dispatch communications by launching an effort to develop a set of standards that would further facilitate interoperability by, for example, adopting a standardized air interface and standardized signaling messages. This effort has become known as the Project 25 initiative.

In 1995, the FCC, in concert with the National Telecommunications and Information Administration (NTIA), established the Public Safety Wireless Advisory Committee (PSWAC) to provide an assessment of the communications needs of public safety through the year 2010. In 1996, the PSWAC released a report setting forth its findings. Among the findings of the report was that 97.5 MHz of new public safety spectrum would be needed by 2010, including 25 MHz within five years (i.e., by 2001).[5]

As a result of the PSWAC report, Congress directed the FCC (in the Balanced Budget Act of 1997) to allocate no later than January 1, 1998, 24 MHz of spectrum between 746 and 806 MHz (to be recovered from television broadcast channels 60-69 as a result of the implementation of digital television (DTV)). Subsequently, the FCC reallocated for public safety use UHF television channels 63, 64, 68, and 69. Later in 1998, the FCC created the Public Safety National Coordinating Committee (NCC) to recommend rules for the use of the new 24 MHz of spectrum in the 700 MHz band. In its final report in 2003, the NCC recommended that one-half of the new spectrum (12 MHz) be designated for urgently needed public safety narrowband voice channels, and that the remaining 12 MHz be designated for wideband data channels. As described later in this Report, significant advances in technology have made it desirable to add the option of using broadband data channels and, to accommodate such use, there are now several new band plans under study by the FCC.

Before turning to the critical features of modern multi-channel trunked dispatch systems, three other points that arise in conjunction with this technological history should be addressed. Each of these three points help underscore that public safety systems have developed on a piecemeal basis tailored to localized circumstances without significant macro-level coordination between different regulators, public safety entities, or regional bodies.

---

[4] The degree of cooperation among agencies required, and the complexity of the administrative issues involved (e.g., in keeping multiple databases operational and current) in these multi-agency agreements should not be underestimated.

[5] FINAL REPORT OF THE PUBLIC SAFETY WIRELESS ADVISORY COMMITTEE (Sept. 11, 1996), *available at* http://pswac.ntia.doc.gov/pubsafe/publications/PSWAC_AL.PDF.

First, the FCC's effort to accommodate the growth of private land mobile radio systems over the years has led to public safety having their allocations or allotments spread over five different bands; namely, Low Band VHF, High Band VHF, UHF, 800 MHz and, as noted immediately above, 700 MHz.[6] Unfortunately, this fragmentation exacerbates interoperability problems and reduces the ability of vendors to achieve economies of scale. Moreover, there are differences in performance among the bands because of radio propagation variations that are associated with the five bands. For example, a jurisdiction in an urban area may prefer a modern digital multi-channel trunked system at 800 MHz where the need for capacity is greatest and shorter ranges can be accommodated. In contrast, a jurisdiction in a very rural area may prefer a High Band VHF analog conventional system where capacity is not a significant issue, maximum coverage from a single site is of paramount importance, and low cost is even more of a factor than in urban areas. In economic terms, it is possible that an optimized local network may be suboptimal from a state, regional or national perspective—e.g., because it exacerbates the interoperability issue and reduces economies of scale.

Second, and related to the first point, the Federal Communications Commission has traditionally licensed private land mobile radio systems, including those used by public safety, on a local, jurisdiction-by-jurisdiction, site-by-site basis. While there may be important benefits associated with such a licensing scheme, it tends to exacerbate the fragmentation discussed immediately above. In addition, as noted before, conventional public safety channels are typically shared with other public safety users and, without the more disciplined approach to channel access provided by a trunked system, there is an incentive for local public safety agencies to acquire and retain their own channels even if they are not heavily used. In the absence of a multi-channel trunked system serving multiple agencies or in the face of a refusal by an individual agency to join such a system (e.g., because a conventional analog system is more economical), opportunities for interoperability, greater spectrum efficiency and larger economies of scale are lost.

Third, in another step to accommodate the growth in private land mobile radio use, the FCC embarked upon a long proceeding to create additional individual channels by decreasing the width of each voice channel from 25 kHz, the current width, to 12.5 kHz (and perhaps eventually to 6.25 kHz). This channel splitting requirement applies to both public safety and industrial licensees in the popular VHF and UHF private land mobile radio bands and the National Telecommunications and Information Administration (NTIA) has adopted a similar requirement for Federal government land mobile radio users. As pointed out in a recent paper, "In an ironic twist of lagging policy, at the same time that users are trying to explain their need for wideband and broadband channels to the FCC, the most heavily used bands in operation are subject to narrowbanding."[7] As discussed later, the requirement to narrowband in the face of much broader industry trends to move to wider channels (e.g., 1.25 – 5.00 MHz) may further exacerbate interoperability problems and lead to further losses in terms of economies of scale.

(3) Essential Features of a Modern Dispatch Oriented Voice Service for Public Safety

---

[6] The FCC recently allocated an additional 50 MHz of spectrum for public safety use in the 4.9 GHz band. However, that spectrum is not included in the discussion here since, with current technology at least, it is not suitable for highly mobile use.

[7] Nancy Jesuale & Bernard C. Eydt, *A Policy Proposal to Enable Cognitive Radio for Public Safety and Industry in the Land Mobile Radio Bands*, IEEE INT'L SYMPOSIUM ON NEW FRONTIERS IN DYNAMIC SPECTRUM ACCESS NETWORKS, Apr. 17-20, 2007.

The focus of this Report thus far has been on public safety voice- and dispatch-oriented wireless communications systems rather than on systems that are capable of handling data, image and video traffic. While systems providing advanced data and multi-media capabilities will be a critical part of public safety's future architecture, the utility of existing systems means that they will not be entirely displaced for some time. For example, even with today's narrowband (i.e., 25 kHz) systems, low speed two-way data communications capabilities are useful for certain applications, such as sending brief, text-based inquiries regarding a vehicle or suspect directly to the National Crime Information Center (NCIC) or other databases maintained by state or local agencies. Meanwhile, the broadband data capabilities of a next generation network will enable high quality images (e.g., mug shots) and video clips (e.g., scenes from a natural disaster location) to be sent between and among public safety units. Despite the large potential benefits of such data communications features, such benefits are less important than speed and reliability in critical "shoot-don't shoot" tactical situations. That is, while having access to building plans and video coverage at a scene may be extremely useful, police officers cannot take the time to create and read data communications messages while pursuing a fleeing suspect. In such situations, nothing takes the place of voice communications with rapid call setup and group calling, thus, such mission critical capabilities must be maintained in the future.

There are two basic scenarios that would allow these mission critical capabilities to be maintained. First, mission critical voice communications (and low speed data services) could be maintained on traditional multi-channel trunked systems optimized for such communications—e.g., Project 25 (P25) systems—while the next generation, common user broadband network would be used to meet advanced data, image and video communications requirements.[8] Second, the mission critical voice communications traffic could be carried "as data" on the converged next generation broadband network assuming it could meet the voice-dispatch requirements.[9] In either case, it is important to understand the current capabilities of modern public safety voice communications systems – especially those that are not normally associated with the ordinary wireless voice communications on existing cellular/PCS systems. In the following two paragraphs, we offer a brief overview of some of the more important capabilities that must be built into a public safety radio system.

As we noted earlier, the *sine qua non* of modern public safety voice communications is rapid voice call setup and group calling. For ordinary voice telephone (landline or wireless) conversations, by contrast, very rapid call setup is not a major issue since it may take tens of seconds for the called telephone to ring and be answered. Because it is an essential issue in mission critical public safety operations, modern systems achieve call setup times of one-half second or less. Moreover, unlike ordinary voice telephony, a dispatch system allows all members of a talk group to receive the transmissions from all other members of that talk-group.[10] In particular, calls to individual units and broadcast calls to all units are possible using such a system.

---

[8] Having two systems—narrowband and broadband—does not necessarily imply the need for each end user two have two devices, because the capability to access multiple systems can be build into a single device. *See, e.g.*, Steve Ellingson & S.M. Shajedul Hasan, *What's in Radio's Future? All-Band, All-Mode Radio Could Solve Interoperability Challenges*, MISSIONCRITICAL COMM., Mar. 2007, at 50.

[9] Many of the Roundtable participants, notably Charles Werner, Chief of the Charlottesville, Va. Fire Department, felt that public safety would wait to migrate their mission critical voice traffic to the NGN until the latter had proven its capabilities to handle such traffic.

[10] Note that group calling is possible in an ordinary voice telephony system by establishing a conference call through a conference bridge but that is not a substitute for the group calling utilized by public safety.

In a modern dispatch system, there can be multiple talk groups and talk group membership can be changed on a dynamic basis to reflect changing operational and tactical needs.[11] Another important capability of modern dispatch systems is a handset feature known as "talk-around" which enables two mobile or portable units to communicate directly with one another *even in the absence of the network infrastructure*.[12] This provides a limited form of fail-safe capability in the event that centralized base station/trunking facilities are out-of-service for whatever reason, or if the two units are out of range of those facilities. The capability can also be used to off-load very local communications from a heavily loaded wide area system. Ordinary wireless telephony services do not offer this capability—no direct, "infrastructureless," "peer-to-peer" communications are possible.

In a modern dispatch system, call requests can be queued when all channels are busy. This is in contrast to the ordinary telephone network where an "all trunks are busy" signal is returned to the user. Because messages are typically much shorter in a multi-channel dispatch system, a channel is more likely to become available in a short time and there is less need to immediately return a busy signal. Moreover, the queuing and associated call processing can provide for priority access (with multiple priority levels) and, in particularly critical situations, for the preemption of calls in progress. More modern systems now offer encryption of public safety communications to provide for greater levels of privacy for critical and often sensitive communications.

To improve or tailor radio system coverage in a given geographic area, modern dispatch systems employ two additional technologies worth noting. First, modern systems are capable of operating in the simulcast mode wherein an additional transmitter is placed in an area needing additional coverage. This additional transmitter simultaneously emits exactly the same signal that is being sent from the main transmitter and on the same frequency. Normally such a transmitter would cause severe interference in the geographic area where the signals overlap. However, by carefully controlling the characteristics of the signals (in terms of carrier frequency and phase or timing) this interference can be minimized. Simulcasting requires that the main and simulcast sites are connected together using a microwave radio link or leased fixed line, but it allows the transmitter or "talk-out" coverage to be optimized without requiring an additional frequency. The second technique deals with the opposite issue—"talk-back" range. Because of their lower power (and associated battery-life issues) and less efficient antennas, the transmit (i.e., talk-back) range of portable, handheld radios is sometimes less than the transmit (i.e., talk-out) range of its associated base station. To compensate for this reduced range in critical areas, remote receivers are often employed in these places. These remote receivers are, in turn, connected back to the base station via a fixed link of some type. When multiple remote receivers are employed, the signal from the remote receiver with the best reception of the signal from the portable is selected. In this situation, the remote receivers are referred to as voting receivers. In combination, simulcasting and remote (or voting) receivers often allow coverage gaps in critical areas to be overcome.

---

[11] With respect to talk groups, an additional feature called late entry is also offered. This feature allows a unit that has just been turned on, or is manually switched from one talk group to another, to join a conversation that is already in progress. That is, it does not need to receive the original signaling message that was used to collect the talk-group on a particular conversation channel.

[12] Talk-around functionality was an area stressed by many of the Roundtable participants. Vice Chair of the National Public Safety Telecommunications Council, Harlin McEwen, emphasized its importance, noting that the key issue of reliability should never be compromised to achieve economies of scale. Moreover, Stephen Meer, Co-Founder and CTO of Intrado Inc., made the point that although talk-around is used as a fall back mechanism in modern systems, capacity issues often preclude its effectiveness in emergency scenarios.

B. Limitations of Modern Public Safety Systems

The characteristics of different generations of public safety communications networks, while not clearly defined, can be roughly identified as follows:

Generation of Public Safety Network	**Early Generation Public Safety Network**	**Later Generation Public Safety Network**	**Current State of Art Public Safety Network**
Type of communications emphasized?	Voice communications	Voice communications	Voice communications with some data
Conventional vs. trunked architecture?	Conventional single channel repeaters	Trunked repeaters	Trunked repeaters
Access method?	Push-to-talk access	Push-to-talk access	Push-to-talk access
Analog vs. digital transmission?	Analog transmission	Analog transmission (but with digital signaling)	All digital transmission
Narrowband vs. broadband?	Narrowband	Narrowband	Narrowband

As reflected above, early generations of public safety networks focused on voice communications, used conventional (i.e., non-trunked) single channel repeaters, used push-to-talk access, and worked in the narrowband, analog transmission mode. Later generations still focused on voice communications, used trunked repeaters, used push-to-talk access, and worked with digital signaling, but continued to use narrowband, analog transmission for the conversation channels. Current generations of state-of-the-art public safety systems (e.g., P25) are still focused on voice communications, but provide circuit switched and packet switched data access that is limited in data rate by the narrowband channels employed. They use trunked repeaters with push-to-talk voice access and employ all digital transmission in narrowband channels. In contrast to the commercial cellular market, the market for P25 systems is much smaller and, in general, is more concentrated and less competitive. Another difference between public safety systems and commercial cellular systems is that the former were designed to provide maximum coverage from each site, thus facilitating simultaneous communications with individual talk-group users spread over a wide area. In engineering terms, these are referred to as noise limited systems and the large coverage areas they produce minimize the number of base stations required to communicate with widely dispersed units and hence reduce the associated fixed infrastructure costs.

Commercial cellular systems on the other hand have evolved over three somewhat more clearly defined generations. First generation (1G) systems were voice oriented, used analog transmission in narrowband (i.e., 30 kHz channels) and employed circuit switching. In the U.S., this generation was exemplified by the AMPS standard. Second generation (2G) systems were still voice oriented, but offered some data capabilities; they were all digital, but still employed circuit switching. Examples of 2G systems included GSM, CDMA, iDEN, and also, in the U.S., TDMA. Third generation (3G) systems on the other hand can seamlessly handle voice, data, image and video traffic, employ packet-oriented switching, and operate in wideband channels

(e.g., 1.25 MHz) allowing high data rate transmission roughly comparable to the speeds achievable by early generation wireline DSL and cable modem services. Examples of 3G systems include WCDMA and CDMA 2000. Moreover, because of the highly competitive environment, the availability of wider channels, and the large manufacturing volumes associated with these systems, their capabilities (e.g., available data rates) continue to increase. The handsets associated with these systems continue to evolve to support not only voice but also data, image, and video or multimedia applications. In contrast to the large coverage areas and noise limited design of public safety dispatch systems, cellular systems are designed to achieve more capacity through the use of smaller coverage areas and intense reuse of each channel. In engineering terms, these are referred to as interference limited systems and are spectrum efficient in terms of handling one-to-one as opposed to one-to-many calling.

From a technical perspective, the current generation of state-of-the-art public safety systems (e.g., P25) does a laudable job of meeting the requirements of rapid voice call setup, group calling among geographically dispersed users, and other specialized narrowband voice and data requirements of the public safety community. However, the narrowband channels and other aspects of the architecture chosen essentially preclude such systems from evolving into broadband networks capable of seamlessly handling voice, data, image and video traffic on a common platform (e.g., the transformation that is already well underway in commercial cellular radio systems). Public safety organizations have identified a pressing need for such broadband capabilities, but current platforms are incapable of providing them.[13]

While it is not a technical limitation *per se*, the market for these specialized multi-channel trunked systems is itself limited by the total size of the public safety market, and by the relatively small purchases made by individual agencies at any given time. This, in turn, limits economies of scale and reduces competitive pressures because fewer suppliers can be supported. The presence or absence of economies of scale makes an enormous difference—consider, for example, that "a cell phone with voice, video, and data capability costs about seven times less than a public safety digital portable radio that cannot even take a digital photo, much less send it to another person."[14] Because of the constraints imposed by the allotted narrowband channels and the specialized nature of multi-channel trunked systems, the public safety community and their vendors cannot directly adopt (a) the commercial cellular technology into the existing public safety bands nor (b) gain appreciably by the economies of scale, competition among vendors, and R&D expenditures that are associated with the commercial cellular marketplace. As another observer noted recently:

> [T]he public safety user community is two orders of magnitude smaller than the commercial user base. As a result, R&D investments in commercial wireless technologies dwarf those made in public safety wireless technologies. In addition, the large size of the commercial market wireless market fosters greater levels of competition between vendors of network infrastructure, user devices, and applications.[15]

---

[13] Testimony of Harlin R. McEwen, Chairman of the International Association of Chiefs of Police Communications & Technology Committee, before the H. Comm. on Energy and Commerce Subcomm. on Telecommunications and the Internet (Mar. 22, 2007), at 4.

[14] Robert Rouleau, *Connecting Data Networks*, PUBLIC SAFETY REP., Aug. 2006, at 98, 102.

[15] Krishna Balachandran et al., *Mobile Responder Communications Networks for Public Safety*, IEEE COMM. MAG., Jan. 2006, at 56.

The higher prices associated with P25 infrastructure and end user devices create still another issue. According to a recent article, a substantial fraction of all public safety systems are still using the same narrowband, analog FM, conventional (i.e., untrunked) systems in the VHF and UHF bands that have been around for decades.[16] Because of the maturity of the technology and the fact that similar two-way radio systems, devices and component parts are used in many different market segments or services in both bands (e.g., in the industrial, transportation, maritime, federal government, and amateur service markets), it is a highly competitive market with multiple domestic and international suppliers. These lower prices, coupled with the propagation advantages associated with the VHF and UHF bands, reduce the incentives for public safety agencies (especially outside the larger urban areas) to deploy modern multi-channel trunked systems thus, as pointed out earlier, aggravating interoperability problems.

In addition to the inability of current narrowband public safety systems to (a) seamlessly offer voice, data, image and video traffic on a common broadband platform and (b) to benefit directly or indirectly from the enormous strides being made in the wideband/broadband commercial cellular market by being confined to a limited ecosystem, the current system, taken as a whole, suffers from both operability and interoperability problems. Operability refers to the ability of communications systems to function effectively, reliably, and continuously; interoperability refers to the ability of different first responders to communicate with one another in real-time, whether or not they are using different communications systems. A broad conception of interoperability, which envisions next generation network-based applications that connect a large number of organizations involved in emergency response, is "the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary . . . utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another . . . in real time, as necessary."[17]

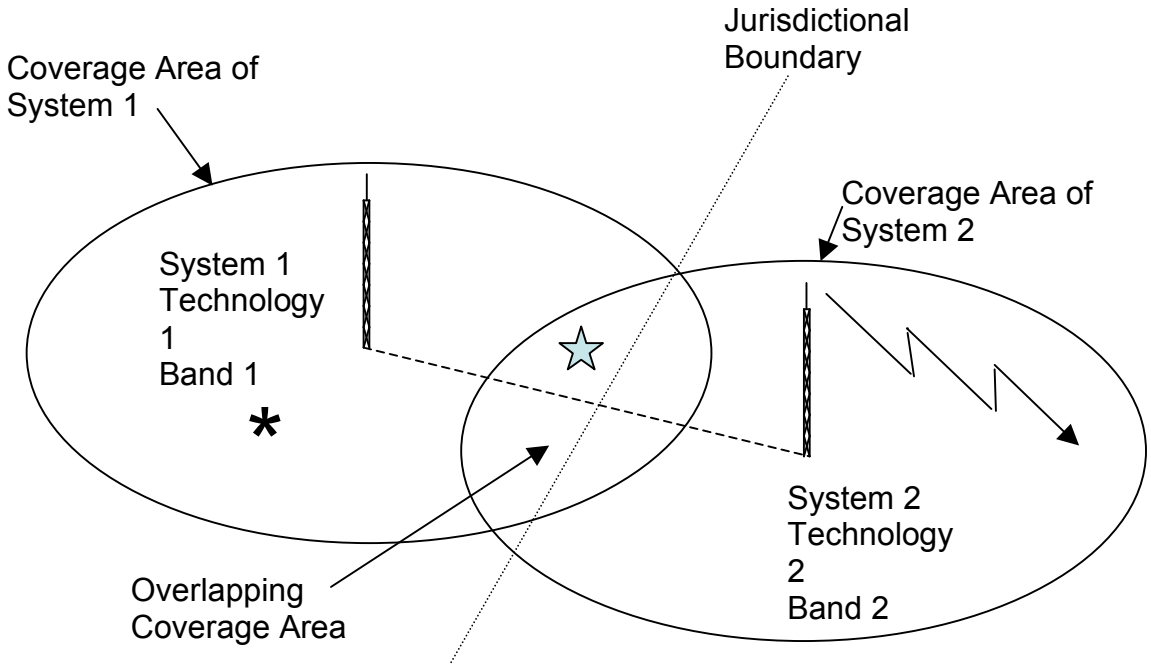
The limitations of current systems in terms of operability and interoperability became woefully apparent during the tragic events of September 11, 2001 and, subsequently, during and after Hurricane Katrina. As previously indicated, the interoperability problem is exacerbated by three principal factors: (1) the policy of licensing public safety radio systems on a local level (indeed, on a channel-by-channel, site-by-site, jurisdiction-by-jurisdiction basis); (2) by historical developments that led to public safety systems being licensed in five separate spectrum bands spanning a range from 25 MHz to 866 MHz; and (3) by the use of a large number of different technologies at the state, local and federal levels of government ranging from legacy FM conventional systems, to proprietary analog and digital multi-channel trunked systems, to modern standardized P25 digital multi-channel trunked systems.

Before turning to the requirements for an NGN for public safety that would address these limitations (namely, the inability to offer seamless broadband connectivity, the inability to directly or indirectly leverage developments in the commercial broadband market, and severe interoperability problems), we will offer a brief overview of the types of solutions that are available for solving or at least reducing the interoperability problem. In doing so, it is useful to distinguish between three parts of a telecommunications network: (1) end user devices; (2) the local access portion of the network; and (3) the wide area or core portion of the network. In a traditional commercial cellular network, the end user devices would be ordinary cell phones, the access portion of the network would include the base stations and microwave or other links for connecting the base stations to the Mobile Switching Center (MSC), and the wide area portion of

[16] Jesuale & Eydt, *supra* note 7, at 3.
[17] H.R. REP. NO. 108-796, at 213 (2004) (Conf. Rep.).

the network would include the facilities used to interconnect the MSCs together and to the public switched telephone network. In a modern P25 public safety system, the end user devices would be mobile and portable radios built to the P25 standard. The access network would include the P25 base stations plus microwave or other links (e.g., telephone company provided leased lines) to connect the base stations to the centralized P25 switch/controller. In addition, if it was a network covering a large geographic area, the wide area portion would include the facilities for interconnecting multiple switch/controller nodes.

FIGURE 2: INTEROPERABILITY SOLUTIONS[18]



Viewed from the perspective presented in Figure 2, interoperability solutions can be divided into the three basic categories—end user device, access network, and core network—described above. In the figure, the circle on the left represents the coverage area of public safety system 1 that is operating in band 1 using access technology 1. For example, public safety system 1 could be operating a multi-channel, P25 trunked system digital access network in the 800 MHz band. The circle on the right depicts the coverage area of a second public safety system that is operating in band 2 using access technology 2. For example, this system could be operating in the UHF (450 MHz) band using conventional analog FM repeaters as the access technology. Note that there is some overlapping coverage between the two systems. Now envision a major emergency of some kind at a location within the overlapping coverage area (marked with a star in the figure). Further assume that the incident is within the jurisdiction of the agency operating system 1, but it is of such a nature that it requires assistance (mutual aid) from mobile units in system 2. This requires the end user devices used by the system 2 units to be able to communicate with the end user devices used by system 1.

[18] Figure 2 is adapted from a slide in a presentation entitled "Interoperability, Public Safety and Homeland Security" by Steve Sharkey, Director of Spectrum and Standards Strategy at Motorola, presented at the Law Seminars International conference on Spectrum Rights and Management, Washington, D.C., Sept. 19, 2006.

Conceptually, interoperability can be achieved in three different ways corresponding to the three categories listed above. First, the arriving mobile from system 2 could utilize a multi-band, multi-mode radio (or a software defined radio equivalent) that is capable of operating on the access network of system 1. This exemplifies an end user device solution. (Such solutions, as we discuss below, are still developing and, at present anyway, have implications in terms of higher cost, weight, and/or lower battery life. In addition, the complexity increases dramatically as the number of modes and bands increase.) Second, while it may be difficult to do in practice, conceptually at least the access network in system 1 could be reconfigured (using software defined radio technology for example) to work with the end user device from system 2 without any changes in that end user device (except perhaps for a change in channels within band 2). This is an access network solution. Third, in this area of overlapping coverage, system 1 units are able to maintain contact with their switch/controller and system 2 units are likewise able to maintain contact with their switch/controller. This means that the wide area or core network connection between the two switch/controller nodes (shown as a dotted line in the figure) could be used with certain functionality within the two nodes to interconnect or provide a "gateway" or bridge between the two systems. This is an example of a network-based solution. If the two switches/controllers use a common standard (e.g., P25) such interconnection is relatively straightforward. It is important to note that while gateway solutions allow conversations on a channel in one system to be heard on another in a second system and *vice versa*, two channels are required to enable this – one on each system. If the traffic is relatively light on the combined channels, spectrum is wasted because a single channel could otherwise handle all of the traffic. On the other hand, if the traffic on the combined channels is heavy, overload and unsatisfactory performance may occur when the two channels are bridged. In short, gateways in general are not always spectrum efficient and, unless other steps are taken, may decrease performance under heavy traffic loads.

The situation changes if the incident is at a point outside the overlapping coverage area. In Figure 2, the asterisk marks such a spot. It is inside the coverage area of system 1 but outside the coverage area of system 2. The first two types of solutions described above—the end user device solution and the access network solution – would still work to provide interoperability. The third solution would not work, because the mobiles associated with system 2 are out of the range of their switch/controller. In some emergency situations, a local, temporary repeater that is compatible with the mobiles associated with system 2 can be located in the vicinity of the incident. A gateway—i.e., network solution—can then be used to bridge the channels together to provide temporary interoperability.[19]

Three concluding comments are in order relating to the technical aspects of interoperability. *First*, narrowband interoperability issues for local first responder personnel would be minimized if every public safety agency used a P25 system operating in the 700 MHz or 800 MHz band. It would also reduce the complexity of achieving interoperability even if the P25 systems operated in different bands because it would facilitate the core network-based

[19] Interoperability problems between two jurisdictions can be minimized by increasing the amount of coverage overlap between the two systems and, indeed, under existing conditions, there are incentives for different agencies to create overlapping coverage to facilitate interoperability in situations requiring mutual aid. However, extending coverage in this way for the sole purpose of facilitating interoperability in emergency conditions can be spectrum inefficient since it reduces the amount of frequency reuse that can be obtained in public safety spectrum allocations/allotments. *See* Jon M. Peha, *How America's Fragmented Approach to Public Safety Wastes Money and Spectrum*, at 8-9, Remarks at the 33rd Telecomm. Pol'y Res. Conf. (Sept., 2005), *available at* http://web.si.umich.edu/tprc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf.

gateway solution. Indeed, there have been some notable successes in terms of deploying statewide, multi-channel trunked systems that address interoperability and reduce the reliance on fragmented, localized systems. But, as noted before, the P25 narrowband technology is a dead-end street in terms of its ability to support broadband applications and its ability to leverage commercial broadband developments. *Second*, gateway or network based solutions—as powerful as they may appear in solving interoperability problems—do have drawbacks and are thus not an efficient (or effective) long term solution. These drawbacks include (a) spectrum inefficiency—taking two or more channels when one would do, (b) the possibility of a decrease in voice quality in translating from one technology or standard to another, and (c) the requirement that both sets of mobiles have access to their respective systems—which may not always be the case especially in rural and remote areas. At the extreme when all of the mobiles and portable units are out of the coverage range of their home systems, the talk-around function as described above in Section A becomes essential, temporary repeater/gateway facilities may need to be deployed, or, in case of isolated areas, access provided to mobile satellite systems (e.g., through a multi-function, multi-band end user device). *Third*, going forward into the broadband world, it should be obvious that there are substantial benefits to deploying systems that are compatible in the first place (especially at the air interface) to minimize the need for gateway or network-based solutions and cost and performance penalties associated with them.

C. Requirements and Other Ingredients for a Next Generation Network for Public Safety

Based upon (1) the discussion in Sections A and B above, (2) the work on next generation public safety systems in other venues such as SAFECOM and Project Mesa, (3) specific proposals that have been set forth by various groups prior to or in conjunction with the FCC's Ninth Proposed Rulemaking, and (4) the related discussions that occurred at the Roundtable, this Section describes the high level requirements and architecture of a next generation network (NGN) for public safety communications. Notably, such a network must interoperate to the maximum practical extent with existing public safety systems and take advantage of cutting-edge technological developments while meeting the specialized needs of the public safety community. Reflecting these two points, the first subsection provides a high level description of the overall architecture of a next generation network (including a brief description of the reasons for relying upon Internet Protocol-based technologies) and the second subsection elaborates upon the more specific public safety requirements and principles that must guide its development.

(1) High Level View of the NGN for Public Safety

Worldwide, both wireline and wireless telecommunications networks are evolving towards a converged, broadband, IP-based network-of-networks capable of supporting voice, data, image, and video applications (including multi-media services) over individual or multiple types of infrastructures.[20] In essence, an NGN for public safety is envisioned as an essential part of that evolution. Notably, the NGN for public safety should be IP-based and capable of handling voice, data, image, video, and multi-media content at up to broadband transmission rates in the core network, and be capable of wirelessly extending those same capabilities to a family of end user devices.

---

[20] TIA TECHNICAL COMMITTEE, NEXT-GENERATION NETWORKS FOCUS GROUP, CONVERGING NGN TECHNICAL FRAMEWORK – ARINCIPLES AND ISSUES (May 30, 2006), *available at* http://docbox.etsi.org/workshop/gsc11/GSC11_GTSC4/gsc11_gtsc4_31%20TIA%20TCNGNFG%20Technical%20Framework_Principles%20and%20Issues.doc.

Before describing the requirements and principles that must guide the development of the NGN for public safety, it may be useful to dwell briefly on the idea that the network should be IP-based. The Internet Protocol (IP) layer of the Internet Protocol suite defines how a packet of information (a collection of bits – be it bits associated with voice, data, image or video content) is organized and structured and then routed on a packet-switched basis over various transmission media. As noted during the Roundtable, a packet of information is sometimes analogized to the standardized shipping containers used in the transportation industry. A standardized container facilitates the shipping and handling of a wide range of goods such as television sets, clothing, and industrial goods on a wide range of transportation infrastructure platforms – e.g., ships, barges, railroad flatcars, and trucks. Similarly, an IP packet can handle the whole range of information types on a wide range of transmission media – e.g., copper wire, fiber optic cable, or wireless.

To appreciate the power of IP-based technology, consider how it can support the transmission of a typical emergency message. In such a network, any standardized packet of voice content can originate in an officer's handset and be delivered over a wireless access network connection and a core network connection (e.g., over an optical fiber cable) to a wired access network (e.g., copper or fiber) connected to a console used by a public safety dispatcher. For systems or devices that are not IP-based, gateways can be provided that, in essence, take the end user information content (and associated signaling messages on the non-IP side) and repackage and convert them to be compatible with the IP-based network on the other side and *vice versa*. To continue the transportation analogy, this would be similar to unpacking a container of TV sets and specially repacking them for transportation over an aircraft that cannot handle the standardized container.

While an IP-based network can efficiently support diverse kinds of traffic, including traffic of disparate urgency and importance, the system must be designed to prioritize and manage the traffic accordingly. This is necessary to ensure that, in the case of mission critical public safety voice communications (as we discuss in the next subsection), the packets of signaling information and content are delivered in a reliable and timely way whether the underlying platform is operated on a private or commercial basis. The technical approaches to achieve this are known, although they are not available in all of today's off-the-shelf IP-based products.

(2) Specific Public Safety Requirements and Associated Principles

We noted earlier that there are two basic scenarios under which the mission critical voice communications needs of public safety could be met going forward. In one, mission critical voice communications (and low speed data services) would be maintained on traditional multi-channel trunked systems optimized for such communications—e.g., P25 systems—while the next generation, common user broadband network would be used to meet advanced broadband data, image and video communications requirements. In the other scenario, the mission critical voice communications traffic would be carried on the converged NGN public safety network along with the advanced data services. At the Roundtable, the consensus was that public safety would wait to migrate their mission critical voice traffic to the NGN until the latter had proven its capabilities to handle such traffic. Because it would be ultimately preferable to handle all traffic—voice, data, image and video—on a fully converged network in order to capture economies of scope, improve spectrum efficiency, and reduce the need for gateways, *it is critical that the requirements for public safety's mission critical voice needs be included in the initial specifications for the NGN for public safety*. These needs include the rapid call setup and group calling capabilities representative of modern narrowband public safety systems as well the other features including

multiple talk-groups, talk-around capabilities, multi-level priority access, preemption and end-to-end encryption for privacy and security described earlier.

Beyond the traditional voice dispatch requirements just described, the NGN public safety system must support a wide range of "data services" or applications which include support for real-time voice connections to the public switched telephone network (PSTN), email and text messaging, high resolution still image and streaming video transmission, internet/internet access to databases, and telemetry transmissions. These requirements have been discussed in depth elsewhere[21] and will not be repeated here. During the Roundtable discussions, however, participants did note that certain bandwidth intensive applications such as streaming video from fixed locations could be off-loaded to other networks, including broadband networks operating in the 4.9 GHz public safety band or other commercial networks.

For reasons discussed in more detail in Section D below, existing public safety narrowband systems will remain in place and a critical component of the public safety communications infrastructure for decades to come. However, the core of the NGN public safety system coupled with appropriate gateways can and should be used to achieve interoperability between (1) the dispatch and other narrowband services provided on the access networks associated with the new NGN system and (2) the dispatch and narrowband data services provided on legacy (e.g., P25) systems. As noted in Part III below, such IP-based solutions for facilitating interoperability are already being offered by vendors such as Cisco, Twisted Pair, and CoCo Communications.

As the Roundtable participants emphasized, an NGN for public safety could allow local agencies to create virtual networks within the larger physical network. In particular, a local jurisdiction could establish its own talk groups and operate what would other otherwise appear as a separate private network during normal times while seamlessly interoperating with other, larger groups of users in emergency conditions. Importantly, this would provide diverse agencies with much of the local control that in the past has been associated with the less interoperable and less spectrum efficient dedicated private systems. This discussion led to the identification of rights management as a critical component in the operation and management of the NGN for public safety. Rights management in this context means, for example, determining who can be assigned to a particular talk group in a particular situation or incident, who makes that decision, and how is it accomplished technically. Similar questions arise in determining who is permitted to place "offnet" calls through the public switched telephone network, whose calls have priority and who can preempt calls already in progress.

Finally, in terms of general principles to guide the development of an NGN for public safety, the Roundtable participants underscored the importance of reliability, security, openness, modularity, extensibility, and reliance on commercial, broadly supported standards. While the importance of the first two is self-evident in the public safety environment, the latter four deserve some elaboration. Openness in this context refers to standards that are open (i.e., available for use by all) and freely available without undue restrictions on their use. Modularity in this context refers to the decomposition of complex hardware/software systems into smaller subsystems

[21] *See, e.g.*, SAFECOM PROGRAM, DEP'T OF HOMELAND SECURITY, PUBLIC SAFETY STATEMENT OF REQUIREMENTS FOR COMMUNICATIONS & INTEROPERABILITY, VOL. I, V. 1.2 (Oct., 2006), *available at* http://www.safecomprogram.gov/NR/rdonlyres/8930E37C-C672-48BA-8C1B-83784D855C1E/0/SoR1_v12_10182006.pdf; PROJECT MESA, STATEMENT OF REQUIREMENTS EXECUTIVE SUMMARY (2005), *available at* http://www.projectmesa.org/MESA_SoR/mesa_sor_executive_summary.pdf.

which interact with each other through well defined interfaces. Modularity (or layering in the protocol sense) coupled with open, standardized interfaces ensures the potential of continued innovation because it facilitates the introduction of new technologies and allows new applications to be developed and deployed without disturbing other subsystems. Extensibility in this context refers to the ability of a system or subsystem to be extended or customized to provide new capabilities. An example of a system that is not extensible is one that does not scale well – that is, its performance in some important dimension decreases if new functionality is added. Because of rapid changes in technology and increasing and more complex demands being placed upon public safety agencies, these goals of openness, modularity, and extensibility are particularly important. Finally, given the probability of continuing budgetary constraints at all levels of government and the enormous amount of resources currently being devoted by the private sector to the development of commercial wireless networks, it behooves public safety agencies to rely, wherever possible, on broadly supported commercial standards—provided they satisfy essential requirements such as security and reliability considerations.

D. Essential Considerations in the Development of the Next Generation Public Safety Network

During the Roundtable, the participants raised a number of practical considerations that will impact on the deployment of the NGN for public safety. These practical considerations included four central points: (1) the network's available coverage; (2) its capacity; (3) its cost and (4) the need to interconnect it with other networks.[22] We discuss each in turn.

As a practical matter, wireless communications networks by their very nature will always suffer from some gaps in coverage. For example, it may be practical to provide reliable "street level" radio coverage in an urban area and to extend that coverage using a variety of specialized techniques such as bi-directional amplifiers, pico-cells, and distributed antenna systems into many buildings. But at some point, "real world" cost constraints prevent coverage from being extended into, to take an extreme case, the third sub-basement of a major bank building. Mark Adams noted, for example, that unless new methods for providing indoor coverage emerge, requiring ubiquitous indoor coverage could significantly increase the cost of a network. Putting aside cost, it may be impossible to gain the necessary access to private property to extend coverage or to test coverage if it is provided external to the building.

A key practical limitation is that it may well be impractical to extend coverage to geographically remote areas using a terrestrial network. While mobile satellite networks can effectively provide "outside" coverage to such areas, again, as a practical matter, it may be impossible to extend satellite coverage into all buildings in such areas or into deep canyons or other locations where the satellites are not visible in a radio sense. Stated another way, obtaining the last few percentage points of geographic coverage becomes prohibitively expensive in any radio-based system designed to cover a wide geographic area. This fact, and the highly variable nature of radio propagation, means that a great deal of care needs to be taken in contractually specifying coverage requirements over a large geographic area, and that some local tailoring of coverage will always be needed to ensure that reliable coverage of particularly critical locations is provided.

[22] These principal considerations assume, as a basic precondition, that the relevant network is built to meet public safety's essential requirements, including rapid call set-up time, group calling, hardened infrastructure, back-up power, etc.

Given a number of real-world constraints, it is also impossible as a practical matter to build a physical or virtual public safety network with sufficient capacity to handle all communications needs—both essential and non-essential—in all locations during a major crisis. Hence priority schemes, load sharing arrangements, and/or methods for screening out non-essential traffic (when the network is in high demand) represent a crucial component of any NGN public safety system. As in the case of radio coverage, reducing the blocking probability (or waiting time in a system where calls are queued) associated with gaining access to a radio channel to extremely low values under extreme load conditions becomes prohibitively expensive. Participants noted that in both cases—coverage and capacity—emergency performance can be enhanced if the end user device, e.g., handset, is capable of accessing more than one network. For example, a multi-mode, multi-band handset could first try a local P25 public safety network, then a terrestrial commercial broadband network, and finally a nationwide mobile satellite network in order to complete a voice call.

Additionally, given public sector funding cycles and constraints, existing public safety narrowband systems will remain in place as a critical component of the public safety communications infrastructure for decades to come. Some narrowband systems may also endure because of some special characteristic such as the low cost of using VHF channels to provide voice and low speed data coverage in remote areas. Moreover, there was a general consensus among the participants in the Roundtable that public safety agencies would be hesitant to migrate their mission critical narrowband voice dispatch traffic until it was proven that the NGN public safety network is capable of meeting their specialized requirements e.g., for providing communications with rapid call setup among geographically dispersed talking groups.

Finally, an NGN public safety network must be able to interconnect with other networks both routinely and in times of crisis. At a basic level, it must be able to interconnect with the ordinary public switched network to allow, for example, a key official with access to an ordinary telephone to communicate (given appropriate permissions) with public safety personnel at the scene of an emergency. Or, at a more advanced level, it should be able to interconnect with a private LMR system utilized by, for example, an electric power utility that has personnel at the scene of an emergency trying to restore critical infrastructure facilities. The participants in the Roundtable noted that the trend of all networks to migrate towards use of the IP suite of protocols should further facilitate such interconnection.

PART II: POLICY STRATEGIES FOR A NEXT GENERATION NETWORK

At the Roundtable, the participants strongly emphasized that emerging technologies, particularly those facilitated by Internet Protocol-based broadband networks, can provide all organizations involved in emergency response with effective and interoperable access to information and real-time communications. The participants also highlighted that a major reorientation of government policy, as well as a fundamental paradigm shift as to how public safety approaches their communications needs, will be necessary to facilitate this next generation architecture. To explain the opportunity for a new policy framework, this Part begins (in Section A) by describing the legacy regulatory strategy and then proceeds (in Section B) to discuss what policy strategies can facilitate the transition to a next generation architecture.

A. The Traditional Policy Paradigm

Only twenty-five years ago, the paradigm users of wireless land mobile radio (LMR) technology were public safety agencies and others who used dispatch networks. At that time, it was difficult to imagine the emergence of widely adopted wireless telephone service—let alone

of wireless broadband access. Indeed, at the time of the AT&T divestiture, AT&T's CEO indicated little to no interest in keeping the newly issued licenses to provide commercial mobile radio service (CMRS). After all, AT&T's McKinsey-commissioned study indicated that only one million or so subscribers would adopt wireless services by 2000. As we all now know, this judgment was only off by a factor of one hundred.

The Federal Communications Commission's paradigm for issuing licenses to operate wireless networks for public safety agencies focused on particular local agencies. In the 1980s, after all, it was accepted wisdom that such networks should be operated on a local basis and even commercial wireless services were viewed as local-based services (and licenses were issued to local firms). Over time, however, the local autonomy of network infrastructure no longer seemed to be the natural way to do things. As discussed in Part I, because the local networks were often assembled using very expensive and proprietary equipment (on account of limited economies of scale), they have often been unable to interoperate with one another.

In general, policymakers have provided local agencies with unconstrained autonomy to use their spectrum licenses to operate local networks as they saw fit. Indeed, until a recent proceeding governing spectrum dedicated to public safety in the 700 MHz band, the conventional policy wisdom was that all blocks of spectrum for public safety should be dedicated to local agencies, with limited requirements to cooperate with other agencies.[23] Similarly, grants in aid to achieve interoperability goals have often been dispensed directly to local agencies, presuming that such agencies would find strategies for interoperating effectively with one another.

Given the traditional paradigm's focus on local networks, spectrum assignments were generally made on a more ad hoc basis and not necessarily with an eye to facilitating a next generation network architecture. Consider, for example, that public safety agencies have received assignments in local VHF and UHF bands, in the 700 and 800 MHz bands, as well as in the 4.9 GHz band. This strategy, while borne of decisions made over decades and the technological realities of an early era, has handicapped the ability of public safety agencies to develop a next generation architecture on at least two fronts—first, not all spectrum is created equal (i.e., the lowest bands and highest bands each have propagation characteristics that limit their utility) and, second, the spectrum dedicated to public safety agencies is not contiguous,[24] making it more difficult to support broadband communications. (More precisely, it is not merely the lack of contiguity that is incompatible with wide-area, broadband networks, but also the fact that channel assignments are channelized into narrow blocks and subject to limited power requirements.) Finally, as Jon Peha has pointed out, the fragmentation of spectrum assignments between local agencies operating local networks is less efficient than a broader network provider, which can better manage its usage of spectrum (through the use of spectrum pooling and trunking, as discussed in Part I).[25] Indeed, the traditional model's requirement of narrowbanding is

[23] The limited exception is the requirements imposed by the frequency coordinators and Regional Planning Committees (RPCs). The Roundtable participants suggested that, while some such entities were effective in spurring cooperation (including on interoperability issues), they have a mixed record on matters outside their core mandate of managing interference.

[24] As Harlin McEwen explained: "Historically, the FCC has allocated individual channels, not contiguous channel blocks, for public safety use. These channels are immediately adjacent to channels allocated for taxicab companies, truck operators, and other businesses. The channels typically are no larger than 25 kHz bandwidth and more frequently 12.5 kHz[.]" Testimony of Harlin R. McEwen, *supra* note 13, at 5.

[25] Jon Peha identifies key ways in which fragmented spectrum assignments result in the inefficient use of spectrum and funding. First, municipalities license spectrum beyond their coverage areas, foreclosing the use of that spectrum by other public safety agencies. Some portion of this reserved spectrum then sits idle. Second, infrastructure must be in place to serve an entire area, regardless of the number of first responders.

increasingly problematic in an era where all communications services are moving on to broadband networks.

It is unfair to policymakers to suggest either that the traditional regime was irrational or that they have failed to move toward a next generation strategy. As noted above, after all, the assumptions of the 1980s justified the approach in place at that time. In the early to mid-2000s, however, it became clear that a new policy strategy was appropriate. To its credit, the FCC has begun to investigate options for using the digital TV transition to spur broader cooperation and federal grants are now conditioned on the development of a statewide interoperability plan (and the establishment of a statewide executive interoperability council). To date, however, neither the FCC nor the Department of Homeland Security grants have galvanized strategic planning and coordination at the regional or state levels to the degree necessary to transform the culture of public safety communications.[26] Moreover, as to the next round of grants (the Public Safety Interoperable Communications Grant Program funded by the auction revenues spurred by the DTV transition), there is a substantial risk that they will similarly fail to spur essential strategic cooperation unless there is some requirement built into the system for the evaluation and dispersal of funds to ensure how they are going to be used.[27] As the GAO concluded, "although DHS has required states to implement statewide plans by the end of 2007, no process has been established for ensuring that states' grant requests are consistent with their statewide plans."[28]

B. Toward A New Policy Paradigm

Thus, deploying a few large systems is more efficient than deploying many small systems. Third, spectrum assignment is limited to distinct channels. As a result, spectrum sits idle when agencies with limited needs are assigned a full channel. Fourth, when agencies do not share spectrum, they must be assigned a sufficient number of channels to ensure that they have enough spectrum even during busy times. Spectrum sharing, on the other hand, means that if one agency is particularly busy, users can switch to another channel. Finally, patching is an inefficient use of spectrum in that it consumes twice the bandwidth to create one communications channel. Peha, *supra* note 19, at 8-9. Similarly, as George Rittenhouse explained in testimony to the House of Representatives:

> Most notably, fragmented use of public safety spectrum and a patchwork of incompatible systems has restrained the development of interoperable communications across geographic regions and among various agencies. Further, it has resulted in inefficient use of spectrum. Accordingly, a shift to public safety networks shared across jurisdictions is necessary to promote interoperability.

Testimony of Dr. George Rittenhouse, Vice President of Technology Integration for Bell Labs at Alcatel-Lucent, before the H. Comm. on Energy and Commerce Subcomm. on Telecommunications and the Internet (Mar. 22, 2007).

[26] Addressing this very issue, the United States Government Accountability Office concluded that, despite the award of over $2 billion in grants from 2003 to 2005, "strategic planning has generally not been used to guide investments and provide assistance to improve communications interoperability on a broader level." UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, FIRST RESPONDERS: MUCH WORK REMAINS TO IMPROVE COMMUNICATIONS INTEROPERABILITY 3 (Apr. 2007), *available at* http://www.gao.gov/new.items/d07301.pdf [hereinafter GAO Report]. As to its finding with regard to specific states, it is clear that the funds dispersed to date have not galvanized states to play an oversight role. Consider, for example, Kentucky where the "[g]rant reviewers at the state level who are in charge of disbursing DHS grant money to localities have had limited means for determining whether funding requests for equipment and training were compatible with statewide interoperability goals." *Id*. at 21.

[27] Testimony of Stephen T. Devine, Missouri State Highway Patrol, before the H. Comm. on Energy and Commerce Subcomm. on Telecommunications and the Internet (Mar. 22, 2007).

[28] GAO Report, *supra* note 26, at 20-21.

The Roundtable participants largely agreed that the traditional policy paradigm is ill-equipped to advance the laudatory goal of facilitating the transition to an NGN architecture. After all, it generally makes sense to operate networks at regional or state levels and to empower local agencies with the ability to use information and communications technology as needed without bearing the responsibility for running advanced networks. Thus, while it is clear that "[n]ew public safety applications and capabilities involving broadband communications, IP technologies and flexible radios and spectrum sharing opportunities with commercial providers where appropriate are all in public safety's future,"[29] it remains to be seen how and when policymakers will spur the transition to a next generation network-based strategy. Fortunately, the spectrum to be made available in the wake of the digital TV transition provides a unique policy opportunity. It is critical that this opportunity not be wasted.

To outline the opportunity for spurring the development of a next generation network, we first discuss two case studies (from New York City and Washington, D.C.) that demonstrate the potential of an NGN in practice. Notably, those two case studies outline the opportunity for government agencies to contract out for the development of an NGN, a model that we sketch out and contrast to its principal alternative, the use of a non-profit body that possesses a license to spectrum and oversees the use of that spectrum as part of a private-public partnership. Finally, after discussing these two models, we explain how a next generation architecture must allow for valuable local flexibility and tailoring as well as overcome cultural obstacles to the adoption of a next generation architecture.

(1) The Next Generation Network in Practice

During the Roundtable, the participants emphasized that next generation networks are not simply a theoretical possibility, but that they are being put into practice in New York City and Washington, D.C. To offer a flavor of the policy issues, and technological opportunities, at the heart of such networks, this subsection discusses these two case studies.

New York City

In September 2006, New York City selected Northrop Grumman for a $500 million, five-year contract to build and operate a broadband wireless network that could be used by all public safety agencies as well as other governmental entities. Using 10 MHz of leased spectrum (reportably in the 2.5 GHz BRS spectrum range), this network will rely on commercially developed technology supported by the international standard UMTS TD-CDMA to facilitate peak data rates of over 2 MB/s to individual users.[30]

The National Capital Region (NCR)

The National Capital Region Interoperability Program (NCR) has developed a plan for constructing a next generation network to serve the District of Columbia and 18 other jurisdictions in Virginia and Maryland.[31] This network, which will use spectrum allotted to

[29] Testimony of Stephen T. Devine, *supra* note 27.
[30] Dave Plank, *Why Not WiMAX*, PUBLIC SAFETY COMM., Apr. 2007, at 33.
[31] *National Capital Region First to Deploy 700 MHZ Wireless Network for Public Safety Communication*, GOV'T TECH., Mar. 2, 2007, http://www.govtech.net/news/news.php?id=104189 [hereinafter *National Capital Region First to Deploy*].

public safety agencies after the digital TV transition (in the 700 MHz band), will be built to meet public safety requirement and promises to deliver its users up to 3.1 Megabits per second and average receiver rates of 1.1 Megabits per second. Indeed, to facilitate the development of this next generation network, the FCC granted NCR a waiver, emphasizing the importance of broadband communications to public safety agencies going forward.[32] To build this network, the NCR contracted with Alcatel-Lucent to "provide a seamless interoperable, redundant wireless broadband network of networks with the capacity to transmit video, data and voice communications."[33]

(2) Two Strategies For A Next Generation Architecture

In this Report, we identify two strategies—"government as contractor" and "public safety spectrum licensee"—for spurring the development of a NGN for public safety. These models, to be sure, are not hard-and-fast distinct approaches, but blur in their application. The essential difference between them is that the latter uses the license itself, which can be used for both commercial and public safety uses, as an incentive for a commercial firm to develop an NGN for public safety. In either case, however, it is critical that the expectations and requirements for a public safety NGN be set forth clearly at the outset and enforced after-the-fact.

Government As Contractor

For both New York City and the National Capital Region, the relevant inter-governmental cooperative effort opted to contract with a "systems integrator" or vendor to oversee and spearhead the development of a next generation system. In the case of New York, for example, the City selected Northrop Grumman to spearhead and oversee the project. The City took upon itself to develop the overall requirements and specifications for the network, but left it to its contractor to ensure that they were satisfied accordingly. (One notable difference between the two efforts is that the New York effort relied on leased spectrum whereas the National Capital Region used spectrum licensed to public safety.)

In general, the government as contractor model can be quite effective. In the United Kingdom, for example, the government outlined the relevant requirements and held a competitive reverse auction for a private firm to bid for the right to build the relevant network and serve public safety agencies for a defined term.[34] If the government defines and enforces the terms effectively, this front-end competition can provide valuable efficiencies and its commitment to a period of years can enable the government to avoid paying all of the capital costs up front. Nonetheless, even if the government need not pay all of the costs up front, this model still requires a significant government investment and, as Harlin McEwen noted, the New York City and Washington, D.C. projects are being built because of the availability of considerable federal funding. Unfortunately, such funding is unlikely to be available for a majority of the nation's public safety agencies.

---

[32] In the Matter of Request by National Capital Region for Waiver of the Commission's Rules to Allow Establishment of a 700 MHz Interoperable Broadband Data Network, *Order*, 22 F.C.C.R. 1846 para. 10, WT Docket 96-86 (Jan. 31, 2007), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-07-454A1.pdf.
[33] *National Capital Region First to Deploy*, *supra* note 31.
[34] Jerry Brito, *Sending Out an S.O.S.: Public Safety Communications Interoperability as a Collective Action Problem*, FED. COMM. L.J. (forthcoming 2007), *available at* http://ssrn.com/abstract=960769 (discussing the U.K. Airwave network).

The government as contractor model is far from perfect and requires thoughtful planning, sufficient funds, and careful oversight to work effectively. On the planning front, governmental entities must not only develop their necessary requirements up front, but also must be mindful of the possibility of vendor lock-in on the applications and equipment side. To the extent, for example, that a particular contract requires the use of proprietary equipment that may well require expensive upgrades, the up front discounts may be deceptive. Moreover, firms might be willing to make commitments that they cannot keep on the back-end, placing a premium on the reputation of the firm as well as the presence of real consequences for a failure to perform effectively.

Public Safety Spectrum Licensee

Over the last year, there has been increasing interest in using a license for wireless spectrum as the incentive for a private firm to operate a network that would be available for public safety needs as well as commercial users. This model could take various forms, including an approach which assigns a portion of the public safety spectrum to a non-profit organization (as the FCC has proposed), an approach which makes spectrum available to a commercial carrier as long as the carrier can meet public safety's requirements (as Jon Peha has proposed[35]), and/or an approach which encumbers some additional band of spectrum with a requirement to serve public safety. At bottom, all of these approaches highlight the logic of a mixed-use network—while public safety requires certain specifications as to its information and communications technology needs, its uses are generally episodic, leaving considerable capacity under-used at most points in time.

By most accounts, the emergence of the public safety spectrum licensee model owes a debt to Morgan O'Brien, whose Cyren Call proposal was built around this concept. More recently, Frontline Wireless has proposed a model with some of the same characteristics and, in response, the FCC has called for consideration of whether a duty to serve public safety via a block auctioned spectrum is a sound policy. Going forward, it is quite possible that variants on this model will emerge and, perhaps, other firms will come forward with new proposals (i.e., other than the Cyren Call and Frontline Wireless approaches). In any event, because a version of this model is being considered seriously by the FCC, it is critical to evaluate how it might spur the development of a next generation architecture.[36]

---

[35] Jon M. Peha, *A New Proposal for a Commercially-Run Broadband System Serving Public Safety*, Comments in the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229, WT Docket No. 96-86, at 4 (Feb. 7, 2007), *available at* http://www.ece.cmu.edu/~peha/safety.html. Under Peha's proposal, the FCC would reassign the license if the carrier did not meet public safety requirements.

[36] This Report does not evaluate the optimal amount of spectrum necessary to facilitate the development of an effective next generation network. One commentator suggested that the entire 24 MHz devoted to public safety agencies as part of the digital transition should be devoted to the development of a next generation system. *See* LARRY IRVING & MICHAEL GALLAGHER, 21ST CENTURY COMMUNICATIONS SYSTEMS FOR FIRST RESPONDERS: THE RIGHT CALL (Nov. 30, 2006) *available at* http://www.digestiblelaw.com/files/upload/WhitePaper.pdf. As a practical matter, this might not be feasible because many public safety agencies have already developed plans or are actually using 12 MHz for their narrowband voice communications. *See* Harlin R. McEwen, *Written Comments and Recommendations*, SOUTHERN GOVERNORS' ASSOCIATION TASK FORCE (Mar. 16, 2007), *available at* http://www.southerngovernors.org/resolutions/InteroperabilityPDF/IACP%20Recommendations%20to%20SGA.pdf. Of course, the Frontline and CyrenCall proposals offered different visions of the necessary amount of spectrum to give rise to such a network and offered different spectrum policy strategies to give rise to that amount. Notably, neither proposal necessarily suggests that public safety needs more spectrum

In its most recent pronouncement on the issue, the FCC has suggested that the licensee of 12 MHz of the spectrum to be made available for public safety after the digital transition be a national not-for-profit entity.[37] Whereas it would require a congressional enactment to allocate more spectrum for public safety uses in the 700 MHz band, the FCC is free to—and is considering—making additional spectrum (say, 10 MHz) available for a public safety-centric network that would be subject to an auction.[38] In theory, the winner of this auction, in conjunction with the 12 MHz dedicated to public safety, could operate a broadband network designed for public safety, but available for other commercial users.

The allure of the public safety spectrum licensee model is that it would use spectrum, in combination with the mixed use concept and public safety as an anchor tenant, as the asset to attract capital investment. There are, to be sure, questions about whether (1) this concept will be economically viable in practice; (2) a network can be built to meet public safety's requirements (including offering prioritization for public safety uses); and (3) such a network will attract private users. Notably, one participant suggested that the spectrum itself was not that valuable and public safety's value as an anchor tenant was limited. Such questions and concerns, however, must be juxtaposed against the question of whether the government will finance a next generation network in the reasonably near future.

In discussing the optimal strategy, many Roundtable participants indicated that the most efficient and cleanest approach to facilitating the development of a next generation network—such as the one built in New York and Washington—would be the direct appropriation of funds (from auction revenues or otherwise) to subsidize it. But to the extent that Congress is unwilling to fund such a program, the question is what second-best option is available. On that score, it is quite plausible that, even with its uncertain success, the public safety spectrum licensee model now under consideration could well be the best strategy for facilitating the development of a next generation architecture—provided that it is implemented in an effective manner that ensured that commitments were kept and abuses were prevented. Notably, as discussed below, the governance challenges to avoid such shortcomings are significant and must be taken very seriously by policymakers.

It is worth noting that the public safety licensee model can work alongside the government as contractor model to the extent that some local, regional, or state efforts might develop a next generation architecture that can be incorporated into the public safety licensee's overall strategy. It is possible, as David Aylward suggested, that there will not be a single top-down national next generation network, but rather some form of allied and compatible "network of networks." Ideally, there will be a formal effort (say, led by the public safety licensee in conjunction with a commercial partner) to support this network of networks. If the public safety licensee initiative fails, it is conceivable that different local, regional, and state-based next generation projects (like the ones in New York and Washington, D.C.) will gravitate toward compatible standards and will be interoperable with one another, but such an achievement will require, at a minimum, some national effort to ensure standardization. Such a result is far from

---

per se, but merely that access to more spectrum at certain points in time is necessary to support public safety's communications needs and the encumbrance of spectrum as a revenue raising tool can facilitate a network build-out.

[37] Ninth NPRM, *supra* note 2.

[38] FCC Addresses Rules Governing Commercial Wireless and Public Safety Licenses in the 700MHz Spectrum Band, *Press Release* (Apr. 25, 2007), http://www.fcc.gov/Daily_Releases/Daily_Business/2007/db0426/DOC-272629A1.pdf.

likely, however, as the history of locally developed systems (which have traditionally adopted incompatible equipment) is quite discouraging on this score.

A critical question related to the public safety licensee model is how the relevant governance structure would work in practice. Presumably, the FCC would license the relevant spectrum to a single entity and, in so doing, approve its governance structure and legitimacy. That entity, in turn, would presumably—either on its own or in conjunction with a firm that purchased an encumbered license (i.e., with a requirement to develop a network in conjunction with public safety)—oversee the development and operation of a next generation network. In proposing this model, the FCC did not offer too many details, but it did suggest that such an entity must be a not-for-profit body and able to represent public safety.[39]

The Roundtable participants agreed that there were notable advantages of establishing such a non-profit board to oversee the development of a public safety NGN, but emphasized that it must be done carefully and that many important issues had yet to be addressed. In terms of the benefits of such a board, there was a clear consensus that it would be more focused on the needs of public safety than could the FCC. At the same time, the participants underscored that the board's charter and membership must be developed thoughtfully so that it could be an effective negotiator and overseer of any commercial contracts to develop an NGN for public safety.[40] First, all agreed that the Board must be fundamentally concerned about and representative of the public interest in general and public safety interests in particular. Second, the Board, either on account of its members or hired consultants, must be technically savvy. Third, the Board must be empowered to act on its own and it is critical that it not routinely need to seek permission of the FCC or be subject to its review (e.g., through an appeals process). Finally, it is important that the Board have a broad perspective, say, including state and local officials mindful of public safety funding and management issues.

In establishing a public safety spectrum licensee who could lease capacity to and cooperate with a commercial provider to oversee the development of the next generation network, it is important that the licensee be well positioned to ensure that the cooperating firm meets its commitments. An effective enforcement mechanism is particularly important to the extent that the commercial firm bid on spectrum licenses that are encumbered with a requirement to serve public safety. The Roundtable did not necessarily identify a single enforcement strategy, but a number of options were suggested, including a performance bond, some kind of lien that would apply to the license purchased at auction, or a lien that would apply to the infrastructure associated with the spectrum intended to serve public safety. A number of participants suggested that enforcement of any such measure be lodged with the Board and not the Commission, as the FCC often is pulled towards accommodation and has yet to develop an a culture that promotes consistently effective enforcement.

One important caution that the Roundtable participants emphasized was that private-public partnerships and public authorities have a mixed track record. In the worst of all worlds, they are sometimes constituted by individuals not up to the job (say, those appointed for purely political reasons) and do not make effective business decisions—often because there is likely little accountability for failure. Moreover, at least in some cases, such bodies are not politically accountable or subject to any oversight, inviting ineffective management, corruption, or other

[39] Ninth NPRM, *supra* note 2, at para. 20.

[40] As Jon Peha explained as to such a body, "Every move it makes will be scrutinized by equipment vendors and potential service providers. Its leadership must be strongly motivated to serve the public interest, while countless Fortune 500 companies try to influence its decisions." Peha, *supra* note 35, at 4.

abuses. In constituting the Board, it is thus critical to build in checks against abuses and that the FCC, in its role as licensor, be mindful of the Board's composition and actions (without being immersed in its decision-making). In particular, the FCC should insist on some form of reporting to ensure a level of transparency and assurance that the spectrum dedicated to public safety is used to facilitate the development of an NGN (which can include leases to commercial providers who will help subsidize the development and deployment of this network).

To underscore the critical nature of an effective enforcement regime, consider the significant cost implications of providing broad ranging coverage in terms of geography and in buildings. As Mark Adams noted, committing to providing indoor coverage can significantly increase network costs. Similarly, to cover all geographic areas can also substantially increase costs because public safety agencies require coverage in all areas, not merely in the ones that are otherwise economical for commercial providers. In short, if commercial providers who gain access to spectrum with a requirement to serve public safety are able to skimp on key requirements without any real consequences, they will have considerable incentives to do so.

(3) The Importance of Flexibility, Adaptability, and Local Tailoring

Through whatever strategies facilitate the development of an NGN for public safety, it is critical that the network allow for local tailoring. In particular, such a network should empower public safety officials to use advanced information and communications technologies to meet their needs without having to operate a network to do so. In effect, each organization using the next generation network would use their own separate Intranet-like, virtual private network that could be tailored to meet their specific needs. Thus, with respect to the applications that are enabled on that network, the types of security provided, and the management of when, how, and by whom the network is accessed, the relevant local official (say, a police chief) will be able to wield the appropriate management authority. Finally, to the extent that a locality wanted additional coverage beyond the level contracted-for or required of the licensed network provider, they would be in a position to pay for it. As a practical matter, however, it is more likely that such a local entity will want to enforce the required level of service rather than pay for additional service.

(4) Challenges for a New Policy Strategy

The development of a new policy strategy must take seriously the need to change the legacy mindset of those operating networks on behalf of public safety agencies. There are, in fact, three distinct cultural legacies that a next generation network must overcome. First, different agencies must be willing to work together and rely on communications technology that they individually do not control. Second, different agencies must agree to shared governance rules that will specify how the next generation network will operate. Finally, public safety agencies must adopt a broader view of communications technology, embracing the idea of a converged ecosystem and letting go of the notion of a specialized network built solely for and operated solely by public safety agencies.

The challenges related to cooperation between different agencies should not be underestimated. As one of us explained previously (quoting Charlottesville Fire Chief Charles Werner):

> the history of fiefdoms within the respective agencies obscures the "gains from cooperation." In many cases, managers of legacy radio systems tell chiefs that "you need to stick with the traditional land mobile radio system" or the system won't

> remain secure. To be sure, education and demonstration projects are part of the answer because there is a basic lack of understanding about how modern networks are designed and managed—for example, security stems from effective encryption, not physically separate networks. Yet education alone will not do the trick. As Chief Werner recounted from his experience, getting beyond the silo-based approach is starting to happen where incentives for cooperation—in the form of federal grants—create opportunities to bring together groups of distinct agencies and individuals through consensus-building leadership.[41]

The concern articulated above is underscored by the experience of the integrated wireless network (IWN), which is being developed for the Department of Justice, the Department of Homeland Security, and the Treasury Department. Notably, the IWN project—at least from the next generation network perspective—is of questionable wisdom insofar as it envisions a nationwide wireless network built for voice communications and is limited in terms of access (i.e., it would not support nor necessarily interoperate with state or local first responders). Given its $5-$10 billion price tag over the next fifteen years, there is a powerful case for scrapping the IWN initiative altogether and folding it into the plans for a next generation network for public safety agencies. Significantly, however, it is not the IWN's limited ambition that has drawn criticism of late, but the inability of the key partners in the project—the DOJ, DHS, and Department of Treasury—to work together. As the Department of Justice Inspector General recently explained, the IWN program was unlikely to be successful both on account of funding failures as well as an inability to develop an effective governance strategy between the relevant agencies.[42] Indeed, on the governance front, the project envisions decisions between the three agencies to be made by consensus, but provides no alternative in the absence of consensus, leading, not surprisingly, to deadlock on some key issues.[43] In general, the Roundtable participants viewed the IWN project as an example of the traditional silo-based culture at work and suggested that a more enlightened strategy would view all emergency responders as part of an enterprise; stated differently, the IWN model not only fails to develop a next generation architecture, it makes the mistake of building separate networks for particular agencies, making interoperability more difficult and leading to higher network development costs.

Once different organizations are willing to work together, there are still challenging governance questions that must be resolved.[44] Notably, the organizations must cooperate based on a shared understanding of how the network will be used, who will have access to it, and how prioritization issues will be managed. In particular, a next generation network will need to develop policies, based on discrete scenarios, which will govern priority access to the network

---

[41] *See* PHILIP J. WEISER, THE ASPEN INSTITUTE, CLEARING THE AIR: CONVERGENCE AND THE SAFETY ENTERPRISE 24-25 (2006), *available at* http://www.aspeninstitute.org/atf/cf/%7BDEB6F227-659B-4EC8-8F848DF23CA704F5%7D/C&S%20FINALAIRSREP06.PDF. To be sure, many others have emphasized the centrality of this issue. *See, e.g.*, SPACE & ADVANCED COMMUNICATIONS RESEARCH INSTITUTE, GEORGE WASHINGTON UNIVERSITY, WHITE PAPER ON EMERGENCY COMMUNICATIONS 1 (Jan. 5, 2006), *available at* http://satjournal.tcom.ohiou.edu/issue10/PDF/Final_Version_White_Paper.pdf (quoting Garry Briese's Dec. 13, 2005 keynote address at the NCEC: "The hardest part of improving emergency warning and recovery efforts is changing human behavior.").

[42] U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL AUDIT DIV., PROGRESS REPORT ON DEVELOPMENT OF THE INTEGRATED WIRELESS NETWORK IN THE DEPARTMENT OF JUSTICE xi (Mar. 2007), *available at* http://www.usdoj.gov/oig/reports/OBD/a0725/final.pdf.

[43] *Id*. at 29.

[44] Tricia Paoletta, counsel for M/A-COM, Inc., noted that the federal government has been active in this area, citing as an example the National Incident Management System (NIMS).

and set forth legitimate usage policies.[45] To some extent, a requirement to pay for services—such as video streaming—will counter any incentives to be a bandwidth hog, but during times of crisis, it may well be the case that all users of the network would insist that they need priority access, or at least some assured access, to the network.

While the challenges noted above are formidable, they are not novel and can be overcome. In particular, some states have already developed governance structures and understandings to enable different agencies to work together effectively. In Virginia, for example, the state has developed a well functioning governance structure to facilitate cooperation on issues ranging from the use of communications technologies to the use of a common language (i.e., moving from so-called "ten-code" abbreviations such as "10-4" to plain English).[46]

Finally, for a next generation network to operate effectively, users must be trained and willing to take advantage of new functionalities and applications. To spur such a willingness, leaders must communicate effectively the advantages of a new network and spur public safety agencies to change their usage habits. To do so, it is likely that officials will need not only to create living laboratories that show how new IP-based technologies can enable public safety agencies to be more effective, but also to provide incentives and build in accountability mechanisms to change the traditional silo-based orientation.[47]

PART III: TRANSITIONAL CHALLENGES

A. Working Within The Current Technological Framework

As discussed in Part II, it is critical that policymakers begin planning today for a next generation architecture. Such plans, however, cannot eclipse the reality that current networks often fail to provide interoperability on a broad basis. As discussed in Part I, the principal effort to facilitate interoperability using the traditional architecture was to encourage the sharing of digital trunked systems and the specialized radio systems. In general, however, this effort succeeded only on a relatively limited basis as the price of such radios has remained very high and many organizations involved in emergency response have never adopted them. Just recently, the GAO summarized the pitfalls of the Project 25 initiative and criticized the Department of Homeland Security for emphasizing this effort in its grant guidance.[48] In retrospect, Project 25

---

[45] Several of the participants, including Charles Werner, Chief of the Charlottesville, Va. Fire Dept., stressed the importance of dealing with governance issues early. In addition, Peter Erickson, CoCo Communications' Vice President of Business Development, noted the example of Texas having three security levels for disaster situations, with full auditing and logging of who was and who was not on the network during any relevant time period.

[46] *See* Chris Essid, *Virginia Puts Interoperability Together*, MISSIONCRITICAL COMM., May 2005, at 70; Chris Essid, *A Model for Interoperability*, MISSIONCRITICAL COMM., Feb. 2007, at 68, 72.

[47] For a fuller discussion of the intergovernmental relations strategy necessary to facilitate the adoption of a next generation network for public safety, see Philip J. Weiser, *Communicating During Emergencies: Toward Interoperability and Effective Information Management*, 59 FED. COMM. L.J. __ (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=980285.

[48] Even at present, as the GAO explained in a recent report:

> [A]mbiguities 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. Nevertheless, DHS has strongly encouraged state and local agencies to use grant funding to purchase Project 25 radios, which are substantially more expensive than non-Project 25 radios. As

made the mistake of treating public safety communications as a distinct island, giving rise to proprietary technologies that are not compatible with commercially developed (and far cheaper) alternatives.[49] As to promoting interoperability, Project 25's progress has "been slow," Harlin McEwen noted, but "recent progress ha[s] been significant." In any event, it is incontestable that Project 25 ultimately focused on narrowband voice communications that fall short in an era where Internet Protocol-based, broadband networks are becoming the preferred mode of communications. Going forward, it is critical that federal and state officials embrace more cost effective and progressive interoperability solutions that are both affordable and future-proof.

The Roundtable participants all agreed that the development of a next generation architecture is going to take time and only will replace existing systems once it is proven out as fully effective.[50] Thus, over the foreseeable future, we are likely to be in a transitional state whereby next generation networks are developed and used alongside their traditional counterparts. By adopting a modular architecture, which might include multi-mode radios, multiple devices, or both, localities can select the best available technologies to meet their needs. Moreover, they should investigate opportunities to provide interoperability on a cost effective basis, realizing that the most effective form of interoperability will be the prevalent use of IP-based, broadband networks.

Even for public safety agencies using traditional land mobile radio systems, a number of firms, including Cisco, Twisted Pair, and CoCo Communications, have developed solutions using Internet Protocol-based technologies to enable interoperability without replacing existing radio systems with expensive Project 25 radios.[51] These solutions have already demonstrated, in deployments such as one in Dallas' Love Field, that they can enable interoperability in a relatively inexpensive fashion.[52] Moreover, with emerging technologies like mesh networking systems, radios connected through such solutions can even communicate directly with one another and without the aid of a central gateway.[53] Finally, such solutions can also, through the

---

> 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. Until DHS modifies its grant guidance to provide more flexibility in purchasing communications equipment, states and localities are likely to continue to purchase expensive equipment that provides them with minimal additional benefits.

GAO Report, *supra* note 26, at 4.

[49] Robert Rouleau, *Connecting Data Networks*, MISSIONCRITICAL COMM., Aug. 2006, at 98, 103.

[50] Mark Adams, Chief Architect, Networks & Communications of Northrop Grumman IT, suggested that we will likely be looking at a ten to fifteen year transition period. On this point, Joe Hanna, former President of APCO, emphasized the importance of not "chopping off" old technologies before new ones were established as reliable and sufficient to meet the needs of public safety. However, Jon Peha, Professor of Electrical and Computer Engineering at Carnegie Mellon University, stressed that even though it will be a long transition period, requirements should be imposed on new technologies to ensure that they eventually replace the legacy systems.

[51] Cisco Systems, *Beyond Radio: Redefining Interoperability to Enhance Public Safety*, *available at* http://www.cisco.com/en/US/products/ps6718/products_white_paper0900aecd80535985.shtml.

[52] Jim McKay, *Instant Interoperability*, GOV'T TECH., Jan. 19, 2007, http://www.govtech.net/magazine/sup_story.php?id=103426&story_pg=1.

[53] *See, e.g.*, Donny Jackson, *Vendor Says New Release Will Deliver Nationwide Interoperable Communications*, MOBILE RADIO TECH., Apr. 11, 2007, http://mrtmag.com/infrastructure/news/nationwide-interoperable-communications-041107/ (noting that, according to CoCo Communications' Director of Technology, Riley Eller, "CoCo has enabled interoperable communications between disparate systems through a mesh-networking protocol that could scale to thousands of digital gateways . . . . With the 4.0

use of encryption technology, address security concerns and even provide users of the system with Type 1 encryption used by the U.S. military.[54] To be sure, such solutions are imperfect, as noted in Part I, but they do offer cost effective alternatives to purchasing new radio systems that are very expensive and technologically inferior to next generation network systems.

Increasingly, states are taking the lead to spearhead cost effective solutions to promote interoperability using traditional LMRs. In Washington State, for example, the State Executive Interoperability Council is promoting the use of a VoIP backbone network to enable state and local agencies using a variety of different radio frequencies to interoperate with one another.[55] To that end, the Olympic Public Safety Communications Alliance Network (OPSCAN), which is using Twisted Pair's WAVE technology, operates a network that provides for interoperability among forty-two agencies and organizations in five counties.[56] Notably, this interoperability occurs among agencies with disparate environments, including VHF, UHF, 700 MHz, and 800 MHz frequencies.[57] Significantly, the IWN network is using a similar technology to address interoperability issues.[58]

In short, during the transition period from today's traditional systems to a next generation system, local agencies should not only adopt interoperability solutions like the ones discussed above, but also use available technologies to supplement their traditional networks. Although sometimes overlooked, the reality today is that many public safety agencies use commercial services and products for a number of purposes.[59] After all, such services are not only quite affordable and user-friendly, but they are increasingly provided according to service level agreements (SLAs) that specify a required level of performance, and that were developed to meet the needs of public safety.[60] Moreover, a number of public safety agencies are already using broadband connections provided by wireless broadband technologies such as wi-fi, EVDO and

---

release, CoCo has improved the scalability of its meshing protocol and designed a system that only resorts to ad-hoc mesh networking when an agency's IP network fails[.]").

[54] Donny Jackson, *Big D's Magic Bullet*, MOBILE RADIO TECH., Mar. 1, 2007, http://mrtmag.com/mobile_voice/mag/radio_big_ds_magic/.

[55] Spencer Bahner & Dave Zehrung, *Interop on the Border*, MISSIONCRITICAL COMM., Nov.-Dec. 2006, at 57, 64.

[56] Case Study, Twisted Pair Solutions, OPSCAN: Helping to Save Lives through Interoperable Communications (2007) (on file with authors).

[57] *Id*.

[58] Wilson P. Dizard III, *General Dynamics to Build Integrated Radio System*, WASHINGTONPOST.COM (Apr. 30, 2007), available at http://www.washingtonpost.com/wp-dyn/content/article/2007/04/29/AR2007042901077.html (quoting Jeff Osman, General Dynamics' executive program manager for IWN, saying that it will use "various types of gateway systems to mix and match the modern digital radio systems with the old-style analog systems that are still used by many police departments nationwide." Osman added that the "federal government study contractor [for the IWN program] recommended an Internet protocol-based solution. It opens up the ability to tie together multiple types of radio systems.").

[59] The DHS National Interoperability Baseline Survey, for example, found that 68% of public agencies use commercial wireless phones on a daily basis, 79% use a personal digital assistant, and 27% use laptop computers and commercial broadband wireless networks. SAFECOM, 2006 NATIONAL INTEROPERABILITY BASELINE SURVEY 45 (Dec. 2006), *available at* http://64.210.244.119/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf.

[60] Justin Schmid, *Upward Mobility*, MISSIONCRITICAL COMM., July 2006, at 44, 51 (noting that over 80% of Verizon Wireless transmission sites in Florida were built with their own backup power generators to enable them to function in case of a power outage during an emergency).

mesh networking.[61] Such systems have enabled public safety agencies to access a range of applications, including photo databases, video camera feeds, and driver's license information.[62]

B. Building A Sustainable Funding Base For Public Safety Communications

At Wal-Mart, there is a widespread appreciation that the investment in information and communications technology has paid great dividends in terms of that firm's ability to operate efficiently.[63] By conceiving of public safety as "an enterprise" that addresses big and small crises, we can equip public safety agencies with cutting edge tools to protect the public. As Harlin McEwen explained, "[o]ur public safety users who should have the best, most advanced, and most robust capabilities too often must rely on systems that are inadequate for their needs today, much less the expanded responsibilities with which they will continue to be charged in the future."[64]

In many respects, the near term presents the most challenging funding demands of all—policymakers must both make do with legacy systems and facilitate the development of a next generation system. Ultimately, once a next generation system is well proven and adopted by public safety agencies, there may well be an opportunity for those agencies to abandon their legacy equipment and, in some cases, traditional spectrum allocations. But such a day is both far off in the future and uncertain. In the meantime, policymakers face the dual challenges of facilitating the development of the best possible technologies to work in conjunction with existing systems as well as laying the groundwork for a next generation architecture.

The funding challenges are often discussed in policy circles as one-time issues related to solving the interoperability problem. Again, the ultimate solution is the effective development and widespread adoption of next generation networks. Like the issues related to the upgrade of the E911 system, however, policymakers have often failed to develop dedicated revenue streams to support public safety's technology needs and, where they have done so, they have sometimes failed to use those funds for their intended purposes.[65]

When discussing proposals like the public safety spectrum licensee proposal, some have emphasized that the spectrum could be monetized to support the development of technology to support public safety communications. This is indeed a virtue of such a strategy, but even this

---

[61] Russell A. Fox & Jennifer A. Lewis, *Whither WiMax*, MISSIONCRITICAL COMM., Mar. 2006, at 48, 51; Mannie Garza, *EnMeshed*, PUBLIC SAFETY COMM., Dec. 2006, at 46-47 (discussing Motorola Mesh Enabled Architecture purchased by the City of Providence); *id*. at 48 (discussing Tropos mesh network adopted by Tucson); *id*. at 51 (discussing PacketHop system); Tropos Networks, *Metro-Scale Wi-Fi for Public Safety: San Mateo Police Department, A Tropos Networks Case Study*, Mar. 2004, www.tropos.com/pdf/SMPD_Casestudy.pdf.

[62] Fox & Lewis, *supra* note 61.

[63] Marc L. Songini, *Wal-Mart Details its RFID Journey*, INFOWORLD, Mar. 2, 2006, http://www.infoworld.com/article/06/03/02/76038_HNwalmartrfid_1.html (discussing some of the benefits of Wal-Mart's RFID system, including tripling the rate of replenishing out-of-stock items).

[64] Testimony of Harlin R. McEwen, *supra* note 13.

[65] *See* UNITED STATES GOV'T ACCOUNTABILITY OFFICE, STATES' COLLECTION AND USE OF FUNDS FOR WIRELESS ENHANCED 911 SERVICES 17-20 (Mar. 2006), *available at* http://www.gao.gov/cgi-bin/getrpt?rptno=GAO-06-338; ALAN G. HEVESI, STATE OF NEW YORK OFFICE OF THE STATE COMPTROLLER, STATUS OF WIRELESS 911 SURCHARGE IN NEW YORK STATE 10 (Feb. 18, 2004), *available at* http://nysosc3.osc.state.ny.us/audits/allaudits/093004/03f9.pdf (finding that between Aug. 2002 and June 2003, more than 40% of funds earmarked for expanding 911 capabilities were diverted for general budget relief in New York State).

approach does not relieve public safety agencies of the need to pay for the adoption of new technologies. After all, such proposals envision that public safety agencies would, at least for the foreseeable future, maintain their traditional LMRs while paying additional funds for access to a next generation network. Consequently, even under this model—as well as, of course, the government as contractor model—there is an essential need for an investment in public safety's use of cutting edge technologies.

C. Develop Clear Requirements, Specifications, and Standards That Will Allow for Entrepreneurship and Flexibility To Meet Public Safety's Needs

How to develop the exact technologies that will comprise a next generation network was a matter that the Roundtable discussed briefly without a clear resolution. By all accounts, any national body interested in promoting a next generation network (or networks) will face the question of how to promote and ensure the adoption of some standardized architecture. At one level, the commitment to use IP-compatible technologies provides an important assurance that all systems will be reasonably compatible (i.e., able to exchange IP packets across a wired backbone). But that commitment does not imply that all mobile devices will be able to communicate with the nearest base station tower, or that applications will work properly across administrative boundaries. An effective public safety communications ecosystem will benefit from a defined family of standards that supports critical applications and encourages a variety of vendors to compete to offer products tailored to meet public safety's needs.

In terms of standardization efforts, there was widespread agreement that Internet Protocol-based technologies would form the basis of a next generation network. Nonetheless, many participants emphasized that there was still a critical need for the public safety community to define the requirements of important applications and for technologies to be adapted to meet those specific needs. Even though, as discussed in Part I, rights management technologies are already widely deployed to enable large enterprise businesses like Wal-Mart to operate a virtual private network with access to a variety of information regulated by rights management,[66] such technologies must be adapted to the public safety context.

The federal government has already started to support the development of next generation standards for public safety, but there is considerable work to be done on this score. Both SAFECOM and National Institute of Standards and Technology (NIST), for example, are involved in an initiative to define how Voice over IP (VoIP) can be used to support public safety, but it is still at a very preliminary stage. Importantly, such standards development efforts need not—and should not—seek to replicate or substitute for commercial development. Rather, as Doug Smith, Executive Vice President and General Manager of Government Solutions of Ericsson, emphasized, they should follow commercial standards activity and highlight what requirements need to be included within the commercially developed standards. Indeed, Smith noted that Ericsson was mindful of the opportunity for public safety agencies to benefit from next generation technology and was already focused on the need for the commercial standards development process to take account of their needs in developing the architecture for next generation network standards.

[66] Such technologies would, for example, enable numerous individuals and firms to have access to Wal-Mart's network, but restrict who has access to employee records, supply chain information, and accounting records. Similarly, a system of rights management in the public safety context would allow all agencies to share an Intranet-like service, but would regulate access to criminal histories to police, medical information to EMS, etc.

The most controversial question related to standards development is whether and, if so, how public safety should embrace a single air interface. Doug Smith of Ericsson stressed the importance of choosing a single air interface, noting that it would render a multi-mode P25/Broadband radio economical. Smith said that without a single air interface, a true multi-mode radio based on multiple standards would not be economical. However, any effort to choose an air interface would risk slowing the development of next generation products for public safety and possibly repeat the failure of the Project 25 initiative to deliver competitively provided and affordable equipment. Consequently, many suggested that the appropriate balance was defining performance requirements, leaving it to the market whether that would be provided via a single air interface. The risk of this approach is that it would require users to purchase multi-mode radios to be assured of ubiquitous coverage. Of course, if chipsets that facilitate multi-mode access were to become less expensive, the excess cost of the multi-mode solution will decline. Nevertheless, the cost of additional modes of operation will never fall to zero, and without standards, it is unclear how many modes each handset must support in order to work effectively in most scenarios. Alternatively, by endorsing a family of air interfaces, public safety could leave some discretion to equipment developers and network operators in a manner that struck a sound balance between standardization and market experimentation. Finally, this debate might become moot as a practical matter to the extent that commercial licensees operating in nearby bands all adopt a particular technology and create huge economies of scale (and a powerful incentive) for public safety to embrace that technology.

D. Support Ongoing Research and Development Efforts That Can Lead to Transformative Technologies

The opportunity for cognitive radio presents dramatic opportunities for a more efficient and effective use of spectrum dedicated to public safety agencies. Notably, policies which embrace cognitive and software defined capabilities represent a logical evolution of spectrum policy trends over the past 25 years.[67] Moreover, in principle, "the flexibility inherent in [software defined radio] technology facilitates multi-protocol, multi-band and multi-service devices that can operate across multiple systems, thereby supporting the 'system of systems' concept for public safety communications."[68] In practice, however, there are still a number of important areas for research and development to resolve, including technical matters (notably, ones related to the development of antennas and security systems), the development of necessary standards, and economic issues (developing a broader base of users to drive the costs down and determining at what point this technology will be cost-effective).[69] To address such issues, policymakers should continue to support research and development of this promising technology, and should also ensure that spectrum policy decisions—such as ones related to a new test-bed for

[67] *See* Brad Bernthal, Timothy X. Brown, Dale N. Hatfield, Douglas C. Sicker, Peter A. Tenhula & Philip J. Weiser, *Trends and Precedents Favoring a Regulatory Embrace of Smart Radio Technologies*, IEEE INT'L SYMPOSIUM ON NEW FRONTIERS IN DYNAMIC SPECTRUM ACCESS NETWORKS, Apr. 17-20, 2007.

[68] SDR FORUM, SOFTWARE DEFINED RADIO TECHNOLOGY FOR PUBLIC SAFETY 26 (Apr. 14, 2006), http://www.sdrforum.org/uploads/pub_36302706_a_0001_v_0_00_public_safety_04_14_06.pdf; *see also* Testimony of Stephen Devine, *supra* note 27 (suggesting that "new frequency agile software based radios, capable of operating on multiple public safety frequency bands, can soon be used as a tool to bridge existing gaps between frequency bands").

[69] *Id*.

experimental uses—enables public safety applications of software-defined radio technology to be tested.[70]

In many cases, policymakers invest solely in a single approach, ignoring the possibility that technological change will create new opportunities. For public safety communications, it is quite likely that even the best version of a next generation architecture strategy will leave open opportunities for different approaches to be tried, such as one based on cognitive radio. As Nancy Jesuale and Bernard C. Eydt suggest, cognitive radio technology, along with a rights management system operated through a trusted providers, promises an effective interoperability solution that can also facilitate broadband access.[71] Moreover, other technologies, such as the use of multiple antenna wireless links, or "MIMO" (multiple-input, multiple-output) communications, deserve serious consideration as MIMO systems provide a number of advantages that can be traded off against one another, including increased coverage, higher throughputs, and improved network reliability.[72] In short, policymakers should both develop today's cutting-edge technologies and invest in the development of tomorrow's technologies that may well yield considerable benefits in the ongoing improvement of a next generation network for public safety.

[70] Comments of the Software Defined Radio Forum in the Matter of Creation of a Spectrum Sharing Innovation Test-Bed (July 10, 2006), *available at* http://www.ntia.doc.gov/ntiahome/frnotices/2006/spectrumshare/sharecomment_007.htm (noting, among other things, that a test bed could provide the basis to evaluate sharing opportunities between adjacent spectrum using shared use technologies).

[71] Jesuale & Eydt, *supra* note 7.

[72] *See* ArrayComm, *An Overview of MAS Principles*, http://www.arraycomm.com/serve.php?page=principles.

PART IV: CONCLUSION

Over the last twenty-five years, three distinct wireless land mobile radio (LMR) networks developed—commercial, state and local public safety, and federal government. In each sphere, the networks largely existed without cooperating with one another, including a lack of shared infrastructure, a reluctance to use technologies developed for the other, and distinct funding models. Internet Protocol-based technologies, however, promises to change that. For public safety agencies, broadband, IP-based technologies can facilitate the development of products and services that can be tailored to meet public safety's requirements, offer them broadband capability and local adaptability, and enable them to leverage ongoing commercial development. In short, such technologies can meet the requirements of public safety agencies without requiring individual public safety agencies to build and operate their own separate networks. They do so by allowing for shared infrastructure and capacity among a large number of users (across agencies and with commercial providers), enabling them to leverage commercially-driven economies of scale and open standards.

In holding the Roundtable, it was remarkable that the participants were able to reach a basic consensus on a number of key points in a debate where overheated rhetoric has sometimes obscured important common ground and concerns. At bottom, there is a broad ranging consensus about the importance of investing in and equipping public safety agencies with the cutting edge information and communications technologies necessary to perform at a highly effective level. Similarly, there was a broad consensus that a new policy model would be necessary to facilitate the development of a next generation network—i.e., local agencies operating their own networks are highly unlikely to facilitate this development. Thus, the most difficult question going forward comes down to the optimal strategy as to different policy tools. In particular, it remains to be determined as what the ideal balance is between relying on government contracting for next generation network development and a public safety licensee model.

The opportunities presented by a next generation architecture promise to enable public safety agencies the ability to communicate effectively with one another and use cutting edge applications that will enable them to do their jobs more effectively. But the transition to this network will take time and will require an ongoing investment of resources. In particular, such a network will not develop overnight, and public safety agencies will need to continue to operate their traditional networks (and make them interoperable) until a next generation network is proven out as an effective substitute for their traditional LMRs.

For America's public safety agencies, the decision to invest in state-of-the art information and communications technology is long overdue. The first step in doing so, however, is for policymakers to realize that this investment is as critical to the success of these agencies as providing them with effective equipment to protect our citizenry and respond to emergency situations across a range of life-and-death situations.

APPENDIX A: SELECTED BIBLIOGRAPHY

- TAMERA CASEY ET. AL., ARCHITECTING A NEXT GENERATION NETWORK FOR PUBLIC SAFETY (Apr., 2006), *available at* http://www.cyrencall.com/downloads/CyrenCall_Technical_Exhibit.pdf.

- PETER CRAMTON ET. AL., CRITERION ECONOMICS, *IMPROVING PUBLIC SAFETY COMMUNICATIONS: AN ANALYSIS OF ALTERNATIVE APPROACHES* (Feb. 6, 2007), *available at* http://www.criterioneconomics.com/docs/Improving_PublicSafetyComm_020507.pdf.

- CLARK KENT ERVIN & DAVID K. AYLWARD, THE ASPEN INSTITUTE, NEXT GENERATION INTER-ORGANIZATIONAL EMERGENCY COMMUNICATIONS: MAKING TANGIBLE PROGRESS WHILE BROADER EFFORTS CONTINUE (2006), *available at* http://www.aspeninstitute.org/atf/cf/%7BDEB6F227-659B-4EC8-8F84-8DF23CA704F5%7D/Homeland_InteroperabilityReport.pdf.

- In the Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, *Eighth Notice of Proposed Rule-Making*, 21 F.C.C.R. 3668, WT Docket 96-86 (Mar. 17, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-34A1.pdf).

- In the Matter of Implementing a Nationwide Broadband Interoperable Public Safety Network in the 700 MHz Band and the Matter of the Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010, *Ninth Notice of Proposed Rule-Making*, 21 F.C.C.R. 14837, PS Docket 06-229, WT Docket 96-86 (Dec. 20, 2006), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-181A1.pdf.

- FINAL REPORT OF THE PUBLIC SAFETY WIRELESS ADVISORY COMMITTEE (Sept. 11, 1996), *available at* http://pswac.ntia.doc.gov/pubsafe/publications/PSWAC_AL.PDF.

- FIRST RESPONSE COALITION, INTEROPERABILITY INNOVATION: STATE BEST PRACTICES & MODELS FOR FIRST RESPONDER COMMUNICATIONS (Mar. 2007), *available at* http://www.firstresponsecoalition.org/docs/FRC_State_Interoperability_Report_030707_FINAL.pdf.

- LARRY IRVING & MICHAEL GALLAGHER, 21ST CENTURY COMMUNICATIONS SYSTEMS FOR FIRST RESPONDERS: THE RIGHT CALL (Nov. 30, 2006) *available at* http://www.digestiblelaw.com/files/upload/WhitePaper.pdf.

- Donny Jackson, *Big D's Magic Bullet*, MOBILE RADIO TECH., Mar. 1, 2007, http://mrtmag.com/mobile_voice/mag/radio_big_ds_magic/.

- Blair Levin et. al., Stifel Nicolaus, *700 MHz: A Pivotal Auction*, WASHINGTON TELECOM, MEDIA, & TECH FOCUS, Mar. 2, 2007, http://www.wcai.com/pdf/2007/700_mar2.pdf.

- Jim McKay, *Instant Interoperability*, GOV'T TECH., Jan. 19, 2007, http://www.govtech.net/magazine/sup_story.php?id=103426&story_pg=1.

- Om Malik, *700 MHz Explained in 10 Steps,* GIGAOM (Mar. 14, 2007),

http://gigaom.com/2007/03/14/700mhz-explained/.

- NATIONAL COMMISSION ON TERRORIST ATTACKS, THE 9/11 COMMISSION REPORT, *available at* http://www.9-11commission.gov/report/911Report.pdf).

- Jon M. Peha, *How America's Fragmented Approach to Public Safety Wastes Spectrum and Funding*, 33RD TELECOMM. POL'Y RES. CONF., Sept. 2005, *available at* http://www.ece.cmu.edu/~peha/safety.html.

- Jon M. Peha, *Fundamental Reform in Public Safety Communications Policy*, Fed. Comm. B.J., 2007, *available at* http://www.mercatus.org/repository/docLib/20061211_Fundamental_Reform_in_Public_Safety_Communications_Policy_-_Peha.pdf).

- Jon M. Peha, *A New Proposal for a Commercially-Run Broadband System Serving Public Safety*, Comments in the Matter of Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229, WT Docket No. 96-86 (Feb. 7, 2007), *available at* http://www.ece.cmu.edu/~peha/safety.html.

- Testimony of Jon M. Peha, before the H. Comm. on Energy and Commerce Subcomm. on Telecomm. and the Internet (Mar. 22, 2007).

- REPORT OF THE 700 MHZ TECHNICAL WORKING GROUP (Oct. 23, 2006), *available at* http://www.npstc.org/meetings/Report%20%20Access%20Spectrum%20and%20Pegasus.pdf.

- Tom Ridge, *Helping First Responders: A Nationwide Public-Safety Network*, WASH. TIMES, June 5, 2006, *available at* http://www.washtimes.com/op-ed/20060604-092821-1278r.htm.

- SAFECOM PROGRAM, DEPARTMENT OF HOMELAND SECURITY, PUBLIC SAFETY STATEMENT OF REQUIREMENTS FOR COMMUNICATIONS & INTEROPERABILITY, VOL. I, V. 1.2 (Oct., 2006), *available at* http://www.safecomprogram.gov/NR/rdonlyres/8930E37C-C672-48BA-8C1B-83784D855C1E/0/SoR1_v12_10182006.pdf.

- SAFECOM PROGRAM, DEPARTMENT OF HOMELAND SECURITY, PUBLIC SAFETY STATEMENT OF REQUIREMENTS FOR COMMUNICATIONS & INTEROPERABILITY, VOL. II, V. 1.0 (Aug. 18, 2006), *available at* http://www.safecomprogram.gov/NR/rdonlyres/B20DC842-B760-4DB0-B3B6-D3F1B0A5F26B/0/PS_SoR2_v10_9112006.pdf.

- SDR FORUM, SOFTWARE DEFINED RADIO TECHNOLOGY FOR PUBLIC SAFETY (Apr. 14, 2006), *available at* http://www.sdrforum.org/uploads/pub_36302706_a_0001_v_0_00_public_safety_04_14_06.pdf.

- Southern Governors' Association--Established an Interoperability Task Force to determine what position the organization should take with regard to proposals to achieve interoperability (For a general description of the Task Force, see http://www.southerngovernors.org/resolutions/Interoperability.html) (For links to all

recommendations and rebuttals filed by interested parties, see http://www.southerngovernors.org/resolutions/InteroperabilityRebuttals.html).

- SPACE & ADVANCED COMMUNICATIONS RESEARCH INSTITUTE, GEORGE WASHINGTON UNIVERSITY, WHITE PAPER ON EMERGENCY COMMUNICATIONS (Jan. 5, 2006), http://satjournal.tcom.ohiou.edu/issue10/PDF/Final_Version_White_Paper.pdf.

- THE SPECTRUM COALITION FOR PUBLIC SAFETY, PUBLIC SAFETY SPECTRUM: HOW MUCH DO WE NEED FOR DATA? (Oct. 25, 2005), *available at* http://www.spectrumcoalition.dc.gov/img/PS_Whitepaper_10-25-05.pdf.

- U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL AUDIT DIVISION, PROGRESS REPORT ON DEVELOPMENT OF THE INTEGRATED WIRELESS NETWORK IN THE DEPARTMENT OF JUSTICE (Mar. 2007), *available at* http://www.usdoj.gov/oig/reports/OBD/a0725/final.pdf.

- UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, FIRST RESPONDERS: MUCH WORK REMAINS TO IMPROVE COMMUNICATIONS INTEROPERABILITY (Apr. 2007), *available at* http://www.gao.gov/new.items/d07301.pdf.

- PHILIP J. WEISER, THE ASPEN INSTITUTE, CLEARING THE AIR: CONVERGENCE AND THE SAFETY ENTERPRISE (2006), *available at* http://www.aspeninstitute.org/atf/cf/%7BDEB6F227-659B-4EC8-8F848DF23CA704F5%7D/C&S%20FINALAIRSREP06.PDF.

- Philip J. Weiser, *Communicating During Emergencies: Toward Interoperability and Effective Information Management*, 59 FED. COMM. L.J. __ (2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=980285.

APPENDIX B: ABOUT THE AUTHORS

Dale Hatfield is an Adjunct Professor of Telecommunications at the University of Colorado and an internationally recognized expert, teacher, and consultant on telecommunications technology and policy. Over his distinguished career in both the public and private sector, he founded a very successful consulting firm and served as the Federal Communications Commission's Chief of the Office of Engineering and Technology, Chief Technologist, and Chief of the Office of Plans & Policy. Professor Hatfield's many honors include: a Department of Commerce Silver Medal for contributions to domestic communications satellite policy, the Attorney General's Distinguished Service Award and the FCC's Gold Medal Award for distinguished service.

Phil Weiser is a Professor of Law and Telecommunications at the University of Colorado and the Founder and Executive Director of the Silicon Flatirons Telecommunications Program. After graduating from New York University School of Law, Professor Weiser served as a law clerk to the Tenth Circuit Court of Appeals Judge David M. Ebel and to United States Supreme Court Justices Byron R. White and Ruth Bader Ginsburg. Before taking his position at CU, Professor Weiser served as the Senior Counsel for Telecommunications Policy to Joel Klein, Assistant Attorney General, Antitrust Division, at the U.S. Department of Justice. Professor Weiser teaches and writes widely on information policy issues and is the author (with Jon Nuechterlein) of "Digital Crossroads: American Telecommunications Policy In the Internet Age (MIT Press 2005)."

APPENDIX C: LIST OF PARTICIPANTS IN THE ROUNDTABLE

Mark Adams
Chief Architect, Networks & Communications
Northrop Grumman IT

Mike Altschul
Senior Vice President and General Counsel
CTIA-the Wireless Association

David K. Aylward
Director
COMCARE-Emergency Response Alliance

Brad Bernthal
Clinical Professor
University of Colorado School of Law

Dean Brenner
Vice President of Government Affairs
QUALCOMM, Inc.

Donald Brittingham
Director - Wireless/Spectrum Policy
Verizon Wireless

JoAnne Dalton
Director of Government Marketing
M/A-COM

Tom Dombrowsky
Engineering Consultant
Wiley Rein LLP

Peter Erickson
Vice President, Business Development
CoCo Communications

Michael Gallagher
Partner
Perkins Coie LLP

Ellen Goodman
Professor
Rutgers School of Law

Robert Gurss
Director of Legal & Government Affairs
Association of Public-Safety Communications Officials International, Inc. (APCO)

Tom Guthrie
President and CEO
Twisted Pair Solutions

Patrick Halley
Government Affairs Director
National Emergency Number Association

Joe Hanna
Consultant and Former APCO President
Association of Public-Safety Communications Officials International, Inc. (APCO)

Dale Hatfield
Former FCC Chief Engineer, Adjunct Professor
University of Colorado

Larry Irving
Principal
The Irving Group

Steven Jones
Executive Director
First Response Coalition

Chris McCabe
Vice President of Regulatory Affairs
CTIA-the Wireless Association

Wanda McCarley
President
Association of Public-Safety Communications Officials International, Inc. (APCO)

Harlin McEwen
Vice Chair
National Public Safety Telecommunications Council

Steve Meer
Co-Founder and CTO
Intrado Inc.

John Muleta
Founder and CEO
M2Z Networks

Morgan O'Brien
Co-Founder and Chairman
Cyren Call Communications

Janice Obuchowski
Chairman
Frontline Wireless

Tricia Paoletta
Partner
Wiltshire & Grannis LLP

Zoran Pavlovic
Director-Strategic Planning
Alltel Communications Inc.

Jon Peha
Professor of Electrical and Computer Engineering
Carnegie Mellon University

Mark Raczynski
Principal Architect, Municipal Wireless
Nortel Business Solutions

Steve Sharkey
Director, Spectrum & Standards Strategy
Motorola

Douglas Smith
Vice President of Network Engineering
Sprint

Douglas Smith
Executive Vice President and General Manager of Government Solutions
Ericsson

A. Lee Swindlehurst
Vice President of Research
ArrayComm, LLC

Neeti Tandon
Principal Member of Technical Staff
AT&T

Peter Tenhula
Vice President, Regulatory Affairs and Business Development
Shared Spectrum Company

Bryan Tramont
Partner
Wilkinson Barker Knauer, LLP

Jill Van Matre
Silicon Flatirons Research Fellow
University of Colorado School of Law

Phil Weiser
Professor of Law & Telecommunications
University of Colorado School of Law

Charles Werner
Fire Chief
Charlottesville, Virginia Fire Department;
International Association of Fire Chiefs