

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of:)	
)	
International Comparison and Consumer Survey Requirements in the Broadband Data Improvement Act)	GN Docket No. 09-47
)	
A National Broadband Plan for Our Future)	GN Docket No. 09-51
)	
Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act)	GN Docket No. 09-137
)	
)	
)	
)	
)	
)	
)	

COMMENTS –NBP PUBLIC NOTICE # 8

COMMENTS OF SKYTERRA SUBSIDIARY LLC

SkyTerra Subsidiary LLC ("SkyTerra") hereby submits the following comments in response to the Public Notice released on September 28, 2009 in the above-referenced proceedings seeking additional comment on public safety, homeland security and cybersecurity elements of the National Broadband Plan.¹ The *Public Notice* seeks comments on a variety of matters organized under four general headings: (1) Public Safety Mobile Wireless Broadband Networks; (2) Next Generation 911; (3) Cyber security and (4) Alerting.

SkyTerra's comments will address several of the matters identified under the first heading, Public Safety Mobile Wireless Broadband Networks. As explained below, no matter how robust, capable or extensive mobile broadband networks become, they cannot provide

¹ *Public Notice, Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of the National Broadband Plan, NBP Public Notice # 8, GN Docket Nos. 09-47, 51 and 137, DA 09-2133 (rel. Sept. 28, 2009) ("Public Notice").*

ubiquitous nationwide coverage, and those networks can be destroyed by many of the same conditions and events (hurricanes, wildfires, terrorist attacks) that create the need for emergency communications in the first place. The FCC should continue to require that “dual-mode” terrestrial/satellite devices be made available to public safety agencies as they adopt mobile broadband services. Only integrated satellite communications capability can ensure that public safety devices will operate in the most remote areas, where no terrestrial networks provide service, and when disasters have disabled terrestrial communications networks.

Background

With over thirteen years of operational experience, SkyTerra offers voice and data to approximately 300,000 units, using a network comprised of its own U.S.-licensed satellite, the Canadian L band satellite licensed to SkyTerra (Canada) Inc., and redundant ground facilities. Public safety users represent a significant portion of SkyTerra’s customer base. SkyTerra provides two-way radio (push-to-talk) and mobile data services to federal, state, and local agencies involved in public safety and emergency response operations. These include, among others, the Federal Emergency Management Agency, the Department of Justice, the Federal Bureau of Investigation, the Louisiana Governor’s Office of Homeland Security and Emergency Preparedness, the California Governor’s Office of Emergency Services, and numerous other local and state fire, police, and emergency response agencies. These public safety entities and first responders depend on SkyTerra’s system for reliable, redundant and ubiquitous wireless services during daily operations and emergencies.

SkyTerra contracted with the Boeing Corporation for the development and construction of two of the most powerful commercial satellites ever developed, providing enough power to offer two-way mobile satellite service to handsets the size of today’s cell phones and PDAs,

servicing as the cornerstone of an integrated satellite-terrestrial network, which will provide ubiquitous wireless broadband services, including Internet access and voice services, in the United States and Canada. These satellites have been built, are being tested, and are scheduled for launch in the 2010-2011 timeframe. The total investment to bring this advanced satellite technology to market is over \$1 billion. Using an all-Internet Protocol ("IP") open architecture, the network will provide significant advantages over existing satellite networks, including higher data speeds, significantly lower deployment and operating costs, and flexibility to support a range of IP applications and services. In addition to integrated satellite and terrestrial L band services, SkyTerra is supporting the development of user device chipsets that will enable the use of its services with terrestrial services in other bands. Specifically with respect to public safety communications, SkyTerra's next-generation network can provide an interoperable overlay and serve as a complement to existing public safety networks while providing advanced features, nationwide coverage, and comprehensive redundancy to the public safety broadband network.

Discussion

As the *Public Notice* requests, SkyTerra's comments follow the organization and structure of the questions presented. SkyTerra also includes two studies and a white paper to provide additional information relevant to the questions asked and incorporates by reference a public safety network cost model it has previously supplied to the FCC.

In particular, SkyTerra urges the Commission to consider the findings of the 2005 white paper, *Toward a Next Generation Strategy: Learning From Katrina and Taking Advantage of New Technologies*, by Dale Hatfield and Phil Weiser ("*Hatfield Weiser Paper*"),² which directly addresses many of the questions posed by the *Public Notice*. The *Hatfield Weiser Paper*

² The *Hatfield Weiser Paper* is included as Exhibit A.

identifies six requirements for a next generation public safety wireless network: ubiquitous access, reliability, interoperability, configurability and security.³

(1)(b)(iv) current and anticipated public safety device needs

The most fundamental requirement for a public safety device is that it must operate reliably when and where a first responder needs to communicate using that device. Public safety devices must “work on” – *i.e.* be compatible with – the network or networks the agencies use day-to-day as well as the networks first responders may need to rely upon occasionally (such as when roaming) or under extraordinary circumstances (such as disaster response when service from primary networks has been interrupted). The devices must be capable of operating on the specific frequency bands and with the various air interfaces and other communications protocols used by public safety networks.

Coverage of the terrestrial public safety broadband network or networks will expand over time, and under even the most optimistic scenarios build out will occur over many years and will never extend to many large areas of the country beyond populated areas and major highways. The only way to ensure that public safety devices are capable of operating over the widest possible area and under extreme conditions, when terrestrial networks are not present or have been damaged, is to equip public safety devices with the capability to communicate with mobile satellite services when terrestrial services are unavailable. The FCC’s rules for the public-private partnership intended to develop a nationwide public safety broadband network in the 700 MHz band contemplate that the D block licensee will be responsible for making available to public safety users at least one device that is capable of operating on both the terrestrial 700 MHz

³ *Hatfield Weiser Paper* at 6.

network and on a satellite network.⁴ In adopting this requirement, the FCC recognized that “satellite technology can provide the only means of communicating where terrestrial communications networks have been damaged or destroyed by wide-scale natural or man-made disasters” and that “satellite services also can enable public safety users to communicate in rural and remote areas that terrestrial services do not reach.”⁵ The Commission should carry this requirement forward and, beyond this minimum requirement, should encourage and facilitate inclusion of seamless satellite capability in a wide range of public safety broadband devices.⁶

In addition, public safety devices must be optimized for the unique requirements of first responders, which are materially different from those of business and consumer uses. As compared to consumer and business devices, public safety devices generally must be more rugged (capable of withstanding extreme conditions), must have longer battery life, and must be more durable (designed and built for a longer service life). Some of these requirements (including more capacious batteries and more durable casings) may result in form factors for public safety devices that differ from those of business and consumer devices providing similar functionality. Obviously, public safety broadband devices must be capable of operating the core applications that the deploying agency demands. However, the nation is in the very early stages

⁴ See *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands*, WT Docket No. 06-150, *Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102, *Section 68.4(a) of the Commission’s Rules Governing Hearing Aid-Compatible Telephones*, WT Docket No. 01-309, *Biennial Regulatory Review – Amendment of Parts 1, 22, 24, 27, and 90 to Streamline and Harmonize Various Rules Affecting Wireless Radio Services*, WT Docket 03-264, *Former Nextel Communications, Inc. Upper 700 MHz Guard Band Licenses and Revisions to Part 27 of the Commission’s Rules*, WT Docket No. 06-169, *Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229, *Development of Operational, Technical and Spectrum Requirements for Meeting Federal, State and Local Public Safety Communications Requirements Through the Year 2010*, WT Docket No. 96-86, *Declaratory Ruling on Reporting Requirement under Commission’s Part 1 Anti-Collusion Rule*, WT Docket No. 07-166, 22 FCC Rcd 15289, ¶ 463-64 (2007) (“700 MHz Second Report and Order”) (“[T]he availability of satellite-based communications capabilities would serve to bolster the availability, robustness, and survivability of public safety communications networks, particularly in circumstances of the direst nature where the safety and security of Americans are greatly at stake.... Accordingly, we require that the D Block licensee make available to public safety users at least one handset that includes a seamlessly integrated satellite solution.”)

⁵ 700 MHz Second Report and Order at ¶ 463.

⁶ See Comments of the MSS/ATC Coalition, PS Docket No. 06-229, filed October 16, 2009.

of public safety broadband network deployment, and it is impossible to predict which applications will be deemed to be essential as public safety agencies' use of mobile broadband matures. SkyTerra expects that some agencies will use broadband devices exclusively to supplement existing voice services, while others will demand unified devices that provide both voice (including push-to-talk) and data services. Beyond voice service, basic data capabilities, and geolocation services, the requirements of agencies are likely to vary significantly. Accordingly, public safety devices should include robust processing and on board storage capability to provide flexibility to host a variety of yet-to-be-developed applications.

Although the specific features required for public safety broadband devices will differ from those of commercial devices, all of the requirements, including seamless satellite access, are likely to be within the capability of device makers with reasonable development time frames.

(1)(b)(vi) specific network features and anticipated architecture that will allow the broadband network to operate seamlessly with disaster recovery capabilities nationwide, and the kind of connectivity needed with legacy and other commercial networks; and

(1)(b)(viii) specific requirements for hardening of cell sites and other network facilities, and for other requirements of network survivability and disaster recovery

As noted above, ensuring that public safety broadband devices operate reliably both *when* and *where* needed requires both network coverage and device capability. Network coverage must be available, and the device must be able to use it. Since conditions on the ground differ from location to location (coverage in urban areas differs from coverage in rural areas) and from time to time (networks are deployed gradually over time, and natural disasters such as fires or hurricanes can disrupt communications networks or sites), public safety broadband devices should be “network agile” – they should be capable of operating on at least two or more different networks.

As explained above, whatever approach the FCC pursues for authorization of the 700 MHz public safety band, the FCC should require that “dual-mode” terrestrial/satellite devices be made available to public safety agencies as they adopt mobile broadband services. Only integrated satellite capability can ensure that public safety devices will operate in the most remote areas, where no terrestrial networks provide service. Similarly, the same disasters that create demand for emergency communications can often destroy or disable critical communications infrastructure in that area. The *Hatfield Weiser Paper* explains that one of the lessons of Katrina is that “failed communications networks emerged as an Achilles’ heel of first responder efforts whereas a bright spot was the use of satellite units that remained effective throughout the tragedy.”⁷ With satellite services, the user device is generally the only network element that exists in the disaster zone, so a working satellite or dual-mode handset can establish a communications link regardless of conditions on the ground. No amount of terrestrial network hardening can provide a comparable level of reliability for disaster communications.

(1)(b)(ix) any studies or other data demonstrating whether and how the requirements needed for urban, suburban and rural environments currently differ and how they are expected to differ in the future.

SkyTerra is aware of two studies providing relevant information in response to this question. A theoretically ideal public safety broadband network would provide ubiquitous, high bandwidth, secure, nationwide, in-building coverage and would be capable of failing over to a backup network when the primary network is unavailable. Costs, logistics and simple practicality dictate that a terrestrial network will not achieve this ideal. Coverage of urban areas is likely to be more robust than coverage of suburban and rural areas, and many remote areas are not likely to receive terrestrial service at all. In urban areas, where many people live and work

⁷ *Hatfield Weiser Paper* at 4.

inside large buildings, in-building coverage is essential. Obviously, in-building coverage is preferred in suburban and rural areas too, but given the relative prevalence of smaller buildings and time spent in vehicles or outdoors in suburban areas, a public safety network should be engineered at least for in-vehicle coverage in suburban areas.

SkyTerra Public Safety Network Cost Model. In 2008 SkyTerra undertook to model a hypothetical nationwide 700 MHz public safety network, in part to help illuminate where the FCC might make practical tradeoffs in performance and coverage with the goal of defining a network that has a realistic probability of being financed and built. SkyTerra presented its findings in comments filed with the Commission, which included its Public Safety Network Cost Model.⁸ The cost of deployment of a terrestrial wireless network depends upon many variables, including, but not limited to, coverage area, available bandwidth, frequency range, re-use criteria, capacity goals, tower or rooftop site availability, selected air interface, level of coverage required (in-building, in-vehicle or outdoor only), specific requirements for site deployment (such as system redundancy), buildout schedule, operating costs during the deployment phase, and many other factors.

SkyTerra's goal in preparing the Public Safety Network Cost Model was to provide a tool that projects the financial impact of certain changes in FCC-mandated performance requirements on the cost of deploying a shared network using the 700 MHz D block and the 700 MHz public safety broadband block. We incorporate by reference the *SkyTerra 700 MHz Comments*, including the Public Safety Network Cost Model. In urban areas, we used in-building link budgets and an area-based "coverage" approach. In suburban and rural areas, we used an area-

⁸ See *In the Matter of Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, WT Docket No. 06-150; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band, PS Docket No. 06-229*, Comments of Mobile Satellite Ventures Subsidiary LLC (filed 20 June 2008) ("[SkyTerra 700 MHz Comments](#)"). We incorporate the Public Safety Cost Model by reference.

based in-vehicle coverage approach to characterize our build, assuming uniform use of 3-sector cells. With more granular data about the performance of LTE now available and with the benefit of other information that has become available since mid-2008, it would be possible to update the model with more current inputs. However, the model was intended as a tool for comparing the relative financial impact of certain regulatory changes and was never intended to reflect the costs of an actual network. For the purpose intended, SkyTerra believes the Public Safety Network Cost Model continues to reflect the relative impact of various network performance requirements on the cost of the 700 MHz public safety network buildout.

Brattle Group/JTC Study on Broadband Adoption by Public Safety Agencies. In July of 2009, SkyTerra commissioned The Brattle Group and JTC, LLC to study the impact of broadband device availability generally, and dual-mode devices specifically, on mobile broadband adoption by public safety agencies. A copy of that report is attached as Exhibit B. The Brattle/JTC report concludes, *inter alia*, that almost 50,000 public safety personnel serve in areas where service is not feasible without dual-mode devices.

In addition, the *Hatfield Weiser Paper* addresses the importance of ubiquitous coverage of territory beyond the populated areas typically covered by commercial terrestrial wireless networks.⁹

(1)(c) concrete, itemized data on costs and resources necessary to satisfy public safety broadband needs for mobile wireless services.

In addition to the costs of building networks, public safety agencies will also need mobile broadband devices designed and built to meet public safety requirements. SkyTerra has undertaken to fund development of device chipsets that will support dual-mode satellite/terrestrial devices, a necessary prerequisite to making such devices available at

⁹ *Hatfield Weiser Paper* at 6-7.

competitive costs. The incremental manufacturing cost of public safety devices with this capability should be less than \$3.¹⁰

However, even with chipsets available, the nonrecurring cost of developing and testing a new public safety class device is substantial. For example, although much work appears to be underway to develop LTE devices for the commercial 700 MHz bands, SkyTerra is aware of no effort by the major chipset vendors to incorporate the 700 MHz public safety broadband spectrum, and this work is a gating factor for any device to be able to operate in the public safety band. SkyTerra understands that the cost of such integration will be approximately \$4 million.

Similarly, even when chipsets that incorporate the public safety bands are available, specific devices meeting public safety requirements must be designed and built. Based on its research, SkyTerra believes that the nonrecurring cost of developing two dual-mode devices for public safety use, one broadband-only handset and one voice-enabled broadband handset, could be as much as \$40 million, with 18 to 24 months required for development and testing.

(1)(g) actions the Commission or other entities must take to ensure interoperability among public safety broadband systems

Disaster response often requires cooperation among multiple agencies, including local, state, and federal responders. Making available a shared, interoperable public safety network, as the FCC has planned for the 700 MHz public safety broadband block and the commercial D block, will facilitate and enhance interoperability among public safety agencies, but it is unlikely to provide full interoperability among all agencies. Today, most state and local public safety agencies maintain their own proprietary wireless networks, and many will continue do to so for the foreseeable future. A ubiquitous satellite component can provide a bridge to the shared network for agencies that have not adopted the 700 MHz network for their primary

¹⁰ See *MSV Ex Parte Presentation*, WT Docket No. 06-150, PS Docket No. 06-229 (filed October 2, 2008).

communications.

The national broadband plan should anticipate a need for some level of interoperability among disparate public safety networks.¹¹ The Department of Homeland Security's *Recommended Federal Interoperable Communications Grant Guidance Fiscal Year (FY) 2008* ("DHS Interoperability Guidelines") provide that interoperability solutions should support "voice communications links between disparate systems: Local, State, Federal emergency responders, including DoD."¹² Widespread availability of dual-mode satellite and terrestrial devices can provide a direct bridge between disparate local, state and federal systems, enabling first responders from agencies at all levels of government to communicate. Many agencies that will not be served by the 700 MHz network already rely on mobile satellite services as an adjunct to their primary networks because of satellite's unique survivability and ubiquitous coverage.¹³ SkyTerra believes that all participants in the shared national network should have access to seamlessly integrated satellite access with the devices they use every day.

¹¹ After September 11, 2001, national policy was changed to require that Federal agencies share information and intelligence with State, local, tribal, and private sector organizations. See, e.g., *Majority Staff Report on Public Health, Safety, and Security for Mass Gatherings*, U.S. House of Representatives Committee on Homeland Security May, 2008, available at <http://homeland.house.gov/SiteDocuments/20080513105623-98169.pdf>. See also, *Hatfield Weiser Paper* at 7-8, 17-18.

¹² *DHS Interoperability Guidelines* at 24, available at http://www.fema.gov/pdf/government/grant/hsgp/fy08_hsgp_safecom.pdf.

¹³ In specifying functional requirements for communications equipment, the DHS Interoperability Guidelines recommend that infrastructure should "allow for communications with various types of user devices (e.g., LMR subscriber units, pagers, cell phones, satellite phones) either through gateways or directly" (p. 23) and that data should provide "seamless roaming and transfer between device types (cellular, satellite, WAN, LAN, WiMax, etc.)" (p. 25).

SkyTerra appreciates the opportunity to provide its comments on this important subject.

SKYTERRA SUBSIDIARY LLC

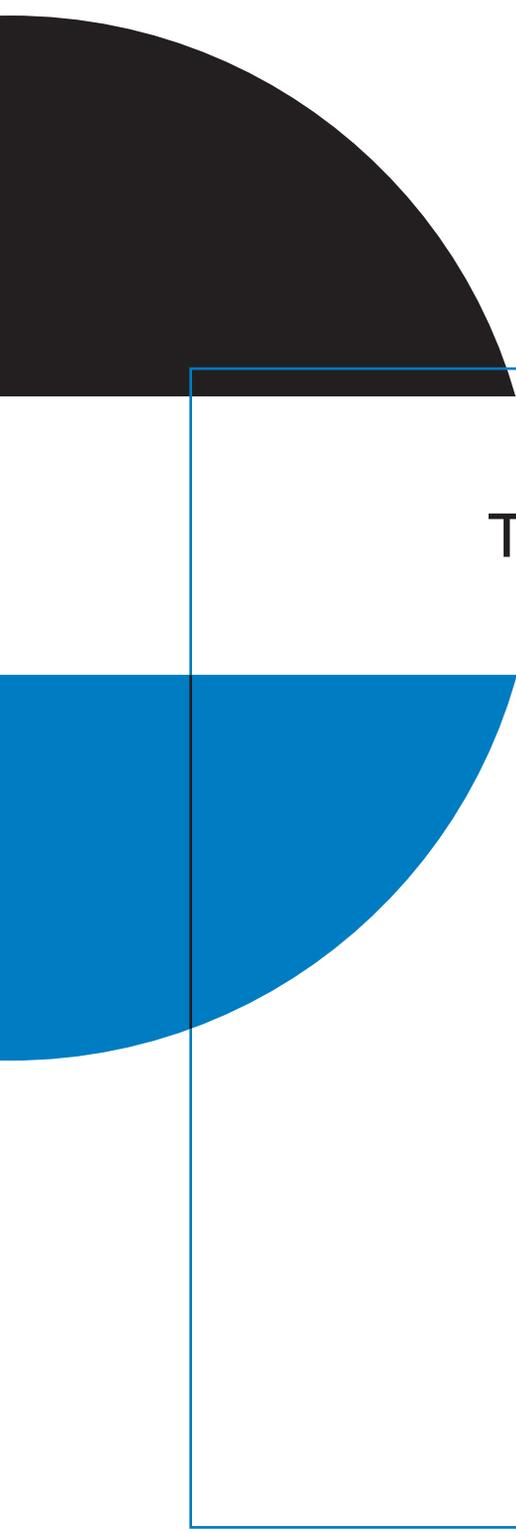
By: _____ /s/

Jeffrey J. Carlisle
Vice President, Regulatory Affairs
SkyTerra Subsidiary LLC
10802 Park Ridge Boulevard
Reston, VA 20191
703-390-2700

Bruce D. Jacobs
John Hane
Pillsbury Winthrop Shaw Pittman LLP
2300 N Street, N.W.
Washington, D.C. 20037
202-663-8000
Counsel for SkyTerra Subsidiary LLC

Dated: November 12, 2009

EXHIBIT A



WHITE PAPER

Toward A Next Generation Strategy:

Learning From Katrina And Taking Advantage Of New Technologies

Dale Hatfield

University of Colorado
Interdisciplinary Telecommunications Program

Phil Weiser

University of Colorado School of Law and
Interdisciplinary Telecommunications Program

EXECUTIVE SUMMARY

In the aftermath of Hurricane Katrina, it appears that a unitary reliance on Land Mobile Radio systems (LMRs) failed public safety agencies, leaving them without any source of communications once their transmission towers went down. Notably, the failure of these agencies—and policymakers more generally—to take advantage of recent technological developments to design a more robust communications system proved to be the Achilles' heel of responding effectively in the wake of a disaster.

As we explain in this White Paper, there is a next generation *architecture* for public safety communications that would bring together existing LMRs, commercial terrestrial services, satellite technology, and wireless broadband systems to provide a robust, reliable, secure, and interoperable broadband communications system. Significantly, the technology exists to make such an architecture a reality; the challenge for policymakers is to provide the leadership to make this important development a reality. To advance this vision, policymakers should ensure that (1) satellite and terrestrial providers are afforded the opportunity—through pro-market and innovative spectrum policies—to develop effective offerings for public safety agencies; and (2) important financial support for public safety agencies promotes this type of a hybrid, next generation architecture.

“[I]n the long term, we will need to learn from this event and work together to improve the reliability, survivability, and security of our nation’s telecommunications networks.”

Joint Statement of Chairman Kevin J. Martin and Commissioner Michael J. Copps Following Their Visit to the Gulf State Region Affected By Hurricane Katrina (September 9, 2005).

I. Introduction

In light of the events and tragic aftermath of Hurricane Katrina, we have revised our earlier White Paper, “Taking A Fresh Look At Public Safety’s Spectrum Needs: Toward A Next Generation Strategy for Public Safety Communications” (prepared on behalf of Mobile Satellite Ventures LP (MSV)¹) to explain how policymakers should respond to rising concerns about breakdowns in public safety communications systems. In assessing the communication breakdowns that appear to have taken place in the wake of Katrina, we observed just the failings noted in our earlier paper—i.e., the relevant public safety agencies lacked interoperable, redundant, secure, and economic methods of communicating with one another. Unfortunately, in the wake of this tragedy, many have advocated the traditionally recommended prescriptions for improving public safety communications (i.e., more dedicated spectrum and more money for upgraded Land Mobile Radio Systems (LMRs)). As we explain, however, both the needs underscored by Katrina and the capabilities made possible by modern technology suggest a next generation strategy of a *flexible architecture* that can incorporate traditional LMRs along with satellite, terrestrial, and wireless broadband systems.

The flexible architecture we embrace is one that will almost certainly be available before the completion of the digital transition and the availability of more spectrum for public safety agencies. In particular, the concept of “multi-mode” radios is already a widespread reality in most segments of the marketplace (except for public safety).² Such multi-mode radios will be even more robust once the recently authorized “**ancillary terrestrial component**” (ATC) of mobile satellite services provides becomes an option for public safety agencies. Even using

¹ MSV is the entity authorized by the Federal Communications Commission in 1989 to construct, launch, and operate a Mobile Satellite Service system in the L-band. MSV’s licensed satellite (AMSC-1) was launched in 1995, and MSV began offering service in 1996. MSV is also the successor to TMI Communications and Company, Limited Partnership (TMI) with respect to TMI’s provision of L-band MSS in the United States. Today, MSV offers a full range of land, maritime, and aeronautical satellite services, including voice and data, using both its own U.S.-licensed satellite and the Canadian-licensed L-band satellite licensed to Mobile Satellite Ventures (Canada) Inc. In November 2004, the Federal Communications Commission authorized MSV to supplement its satellite service with ATC. See Mobile Satellite Ventures Subsidiary LLC, Order and Authorization, DA 04-3553 (Chief, International Bureau, November 8, 2004).

² See, e.g., Mike Dano, LG, *Qualcomm Release Dual-Mode Technology*, RCR Wireless News (September 23, 2005) (www.rcrnews.com/printwindow.cms?newsId=24251&pageType=news) (discussing latest multi-mode technological developments).

traditional satellite technology, firms like MSV are able to provide service to a number of public safety agencies today. But beginning within the next couple of years, after completing the deployment of an ATC service, MSV (and perhaps others) will be able to expand this service and offer it more efficiently to public safety agencies across the United States and provide it as a critical part of a realistic and effective nationwide interoperable broadband mobile communications system for public safety agencies. Such a convergence between wireless and satellite is already becoming a reality in other countries, such as South Korea, meaning that its prospects in the United States will depend on whether the market appreciates the benefits of a built-in satellite backup, not on whether the product is technically feasible.³

This White Paper proceeds in four parts. First, we review the events around Hurricane Katrina and underscore how public safety communications systems failed to operate effectively. Second, we outline the requirements for an ideal public safety network, noting the often cited shortcomings of traditional commercial providers. Third, we explain how public safety agencies can utilize networks provided by commercial providers—particularly hybrid satellite and terrestrial systems—to satisfy the relevant requirements in a cost-effective fashion. Finally, we explain how policymakers can facilitate the transition to such optimal hybrid networks.

I. Katrina and Its Lessons

The aftermath of Hurricane Katrina, when many mission critical networks were down and unavailable to key governmental officials and first responders, made clear that effective communication during a crisis should not and cannot be a luxury. In particular, if mission critical networks do not live up to their name—i.e., are not reliable, survivable, and secure—first responders will be left unable to perform their job effectively. In the case of Katrina, public safety agencies realized that traditional Land Mobile Radio Systems (LMRs)—even along with commercial wireless systems—are unlikely to remain widely available under certain adverse conditions. As Federal Communications Commission (FCC) Chairman Martin emphasized, “[i]f we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications.”⁴

³ Katrina Could Unite Wireless, Satellite Industries, Communications Daily (September 22, 2005).

⁴ Statement of Kevin J. Martin, Hearing on Communications in A Disaster 7 (September 22, 2005).

As many accounts have reported, Hurricane Katrina left Louisiana's governmental communications systems in shambles. Governor Kathleen Blanco reported early on that wireless networks throughout the state were down and that many state officials were cut off from communicating with one another. As Reuters put it, "[t]he collapse of the communications network in the New Orleans area has been widely blamed for contributing to the disaster there, as local officials were unable to talk to each other and to federal authorities to arrange relief in the days after Katrina laid waste to the city."⁵

Based on preliminary reports, it appears that failed communications networks emerged as an Achilles' heel of first responder efforts whereas a bright spot was the use of satellite units that remained effective throughout the tragedy. Keith Sims, the telecom chief of Tampa Electric who brought a team to New Orleans to help repair the damage, explained that "[c]ellphones don't do much good after a hurricane" whereas satellite units worked very well in the storm's aftermath. As another user of satellite technology put it, "it's the only way [our employees] can talk to one another."⁶ Noting that satellite systems remained intact during the crisis, FCC Chairman Martin explained that they "helped to bridge the gaps left by outages by providing satellite phones and video links to law enforcement, medical personnel, emergency relief personnel, and news outlets."⁷ In sum, as one trade publication explained, "[a]fter Hurricane Katrina wreaked havoc on the Gulf Coast terrestrial wireless network, satellite phones and satellite data services played a critical role in filling communication gaps left by the storm."⁸

⁵ Wireless Carriers Reconnect in New Orleans, CNET News.com (September 4, 2005) (http://news.com.com/Wireless+carriers+reconnect+in+New+Orleans/2100-1039_3-5849066.html); see also Mimi Hall, *Hard Lessons of Katrina Being Put to Immediate Use*, USA Today 1A (September 22, 2005) ("When Katrina wiped out communications along the Gulf Coast, officials and key emergency workers were cut off from each other. That contributed greatly to the chaos on the ground.").

⁶ Paul Davidson, Satellite phones provide critical link to outside world, USA Today (September 5, 2005) (http://www.usatoday.com/tech/wireless/2005-09-05-satellite-phones_x.htm?POE=TECISVA); see also Press Release, State Wildlife Agency Playing Large Role in Hurricane Relief (September 6, 2005) (<http://www.mdwfp.com/Level1/NewsRoom.asp?ID=302>) (explaining that satellite units provided a critical means of communicating with one another, enabling different relief efforts to work together).

⁷ See, e.g., Statement of Kevin J. Martin, Hearing on Communications in A Disaster 3 (September 22, 2005).

⁸ Katrina Could Unite Wireless, Satellite Industries, COMMUNICATIONS DAILY (September 22, 2005).

Along with other providers of mobile satellite services, MSV offered crucial assistance to governmental organizations in the affected area. As MSV CEO Alex Good related to FCC Chairman Martin, many satellite terminals were being used to provide access to reliable, quality communications for agencies ranging from the American Red Cross, the Federal Emergency Management Agency to the Louisiana Department of Homeland Security. Even with MSV providing access to these terminals at cost and providing free airtime to state and local public safety agencies in the affected area, the economics of such devices do not lend themselves to widespread use (i.e., terminals costing thousands of dollars and air time in the several dollar a minute range)—thus leaving many first responders cut off from crucial communications.

Based on currently available information, a central lesson underscored by Katrina is that relying solely on Land Mobile Radios (LMRs) does not provide the reliability and survivability sometimes suggested by its boosters. In particular, some have claimed that governmental systems that are maintained by public safety agencies and protected in ways that commercial networks are not would be sufficiently robust to continue operating during an emergency. Such claims, however, generally focus on a particular threat—traffic from ordinary users overwhelming the network. Other claims about commercial systems—say, the need to provide backup power, enable re-charging of the handsets, and the lack of coverage in some areas—may prove problematic in certain cases. Nonetheless, an optimally designed system (i.e., a flexible one allowing the use of satellite technology and multiple networks) can provide the greatest assurance that public safety communications will remain available during a time of crisis.

In short, it is essential that mission critical networks be able to survive natural or manmade disasters so that first responders can perform their role effectively. Katrina reminds us that LMR systems can be destroyed even when protected by some measures not used by their commercial brethren, underscoring that the best assurance of survivability is the use of a flexible system that includes satellite technology. As we discuss in Part II, the flexibility and redundancy of system that includes satellite technology is one only of a number of requirements that we believe are important for a next generation public safety communications system.

II. Requirements For A Next Generation Public Safety Communications System

In the wake of 9/11 and Katrina, combined with an emerging awareness of the shortcomings of current public safety communications networks, most policymakers are familiar with the arguments for developing a next generation (i.e., broadband and interoperable) mobile radio network. Thus, rather than focus on the particular applications and rationale for such a network, this Part explains the key requirements of any such network. In particular, we explain the need for (A) ubiquitous access; (B) reliability; (C) interoperability; (D) configurability; and (E) security. In so doing, we make a special effort to acknowledge the criticisms traditionally leveled at commercial wireless providers.

A. Ubiquitous Access

A fundamental requirement for public safety mobile radio networks is that they must function in all areas served by first responders. The need for ubiquitous access is a notorious shortcoming of modern commercial mobile radio networks, which often do not serve more remote areas.⁹ As commercial providers underscore, the territory they do serve often includes 90% of the population. Because of the increasingly urbanized nature of the nation, however, this coverage can be achieved while covering less than 10% percent of the U.S. land area. Given this limited geographic reach and the lack of coverage for the other 10% of the population, public safety agencies traditionally have eschewed reliance on commercial systems and have developed their own land mobile radio (LMR) systems. Significantly, even many LMR systems operated by public safety agencies do not cover their entire territory. The New Mexico State Police's system, for example, cannot reach 15% of the state—and is limited to voice communications.¹⁰

The second aspect of ubiquitous coverage involves ensuring service in buildings. Historically, the lack of radio communications ability within buildings represented a notable failing of public safety LMRs—and one that has led to tragic results during emergency situations such as 9/11.¹¹

⁹ Mary Greczyn, *FCC Weighs Whether To Scrap 20-Year-Old Cellular Mandates*, COMMUNICATIONS DAILY (August 7, 2002) (reporting that digital cellular networks reached only around 50% of the population).

¹⁰ James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (<http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf>).

¹¹ *Increasing FDNY's Preparedness*, August 19, 2002 (www.nyc.gov/html/fdny/html/mck_report/toc.html).

To respond to this failing, some cities have required in-building coverage plans as part of any new construction (such as the installation of bi-directional amplifiers). In-building systems can be expensive, however, with major high rise buildings requiring an investment of \$1-\$2 million.¹²

B. Reliability

For public safety agencies, the second critical requirement is that “mission critical” networks be able to survive and continue to operate during natural or man-made disasters, such as hurricanes, earthquakes, fires, or a high-powered blast caused by a bomb. In many cases, traditional commercial networks are not engineered to withstand such disasters—either because they are not protected or because they do not have sufficient generation capacity or battery back-up to stay online if the power grid goes down. Moreover, even if available, commercial systems are often overloaded by calls during emergencies; as one report explained, “[e]xperience has shown that such systems are often the most unreliable during critical incidents when public demand overwhelms the system.”¹³ Tragically, as Katrina reminds us, disasters can destroy all available terrestrial systems, meaning that the only way to assure reliability and available access is to incorporate a satellite component. In short, through some combination of public or commercial wireless and satellite systems, it is clear that public safety agencies need access to a system that will remain operational and available during emergencies and that will afford them with priority access.

C. Interoperability

As numerous policy observers and policymakers have emphasized, the lack of interoperability among public safety agencies remains a grave concern.¹⁴ As the Federal Communications Commission has defined the issue, interoperability is “[a]n essential communications link within public safety and public service wireless communications systems which permits units from two or

¹² Public Safety Wireless Network Program, *Public Safety In-Building/In-Tunnel Ordinances and Their Benefits to Interoperability Report* (November 2002) (http://www.safecomprogram.gov/NR/rdonlyres/2311FAAD-18DE-4EA9-BC5A-6C99CC24BAFA/0/In_Building_In_Tunnel_Ordinances_Report.pdf).

¹³ National Task Force on Interoperability, *When They Can't Talk, Lives Are Lost* (February 2003) (http://www.agileprogram.org/ntfi/ntfi_brochure.pdf).

¹⁴ See, e.g., Government Accountability Office, *Protecting Structures and Improving Communications During Wildland Fires 24* (April 2005) (<http://www.gao.gov/new.items/d05380.pdf>) (“The lack of communications interoperability among firefighting and other first-responder agencies can impair their ability to respond to emergencies quickly and safely, and cost lives among responders and those they are trying to assist.”).

more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results.”¹⁵ Stated more simply, interoperability means that two (or more) emergency service providers—say, a paramedic and a fire fighter—can communicate with one another in an efficient, reliable, and secure fashion. Given the American system of government, with thousands of local agencies that enjoy local autonomy, it should not be surprising that different jurisdictions (as well as, unfortunately, agencies within the same jurisdiction) have often made decisions that inadvertently do not promote this goal.

In looking back at the numerous inquiries into the causes of the continuing lack of interoperability, several themes emerge as predominant. First, many jurisdictions lack the funds to upgrade their systems (some often 20-40 years old) and, more fundamentally, are unable to plan effectively for their wireless communications needs. Second, local public safety administrators (either managers like the Chief of Police or the relevant IT professional working in an agency) are often attached to their current approaches and unwilling to give up control to facilitate a greater sharing of resources and technology—an understandable concern where they are responsible for ensuring that communications systems work effectively. In this respect, achieving interoperability is not simply a matter of upgrading equipment, but also of changing the culture of operating in isolation and without full regard for how other public safety agencies operate. To be sure, there are some notable successful ventures that have galvanized regional cooperation between different agencies, such as the Capital Wireless Integrated Network (CapWIN) project that has brought together over 40 local, state, and federal public safety agencies in the Washington, D.C. metro area into a system that provides important real-time communication abilities and access to government databases. Such projects, however, require a system of effective governance involving a number of discrete agencies willing to coordinate their radio equipment needs. Notably, as many other failed initiatives demonstrate, ambitious visions of developing a single system to be used by all relevant agencies are very difficult to achieve and thus more flexible approaches are far more likely to be successful.¹⁶

¹⁵ *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 ¶ 76 (1998).

¹⁶ National Task Force on Interoperability, *Why Can't We Talk: Working Together to Bridge The Communications Gap to Save Lives, Supplemental Resources 19-22* (February 2003) (http://www.agileprogram.org/ntfi/ntfi_supplemental.pdf) (detailing Colorado's failed approach).

A third major cause of limited interoperability is that many agencies cannot communicate with one another because they use equipment with incompatible (and often proprietary) technology. In some cases, these sorts of challenges can be addressed by developing intermediary patches—i.e., a dispatch center (using “bridge equipment”) that can interconnect different systems—but such “second best” solutions are expensive and inefficient compared to more rationally designed systems.

Although none have taken hold completely, there are a number of efforts that have attempted to overcome the lack of common standards and to develop ones to facilitate interoperable public safety communications. Notably, the APCO-sponsored Project 25 standard and the European-developed TETRA standard have both sought to advance this goal; more recently, the international “Project MESA” initiative has begun to develop a next generation standard. As for the exchange of data, a coalition of first responders is now working to develop an Extensible Markup Language (XML)-based standard (i.e., the Emergency Data Exchange Language (EDXL)) to enable the panoply of different agencies that might be called to the scene of an accident (i.e., public safety, transportation, and medical personnel) to share information with one another¹⁷ In its effort to facilitate interoperability, the Federal Communications Commission chartered an advisory committee (the Public Safety National Coordination Committee) that has recommended technical and operational standards for spectrum that will be made available to public safety agencies.¹⁸ Finally, the Department of Homeland Security’s SAFECOM initiative has developed a “statement of requirements” that, in the words of SAFECOM’s Director, provide an “architectural framework for future interoperable public safety communications.”¹⁹

The final cause of limited interoperability is that local public safety agencies often lack access to (or may not choose to use) radio spectrum in the same frequency bands used by sister

¹⁷ Diane Frank, *First Responders Seek Common Lingo*, FEDERAL COMPUTER WEEK (March 15, 2004) (<http://www.fcw.com/article84556>).

¹⁸ See *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, Fifth Memorandum Opinion and Order, ___ FCC Rcd ___ (2005) (considering recommendations).

¹⁹ Press Release, Homeland Security First to Define Interoperability Requirements for Nation’s First Responder Community (April 26, 2004) (<http://www.dhs.gov/dhspublic/display?content=3513>).

agencies. As a result, public safety agencies—which use any one of ten different bands of spectrum—often cannot communicate with one another even when using compatible technology. To rectify this situation, many in the public safety community have suggested that the transition to digital television, which will open up 24 MHz of spectrum in the valuable 700 MHz band for public safety uses,²⁰ should alleviate such concerns. But, to understate matters, it remains “somewhat elusive” whether the transition will be completed by 2006—or even 2009, for that matter—and “no public safety agency can logically budget for equipment that uses radio spectrum that is not yet available for them.”²¹

In evaluating the spectrum issue, it is important to make clear that this aspect of interoperability might be unsolvable because different agencies often have good reasons for choosing different bands. In short, there are big differences in propagation characteristics between the lowest frequency band and the higher frequency bands used by public safety agencies; consequently, agencies in, say, mountainous areas have compelling reasons for choosing different bands than those agencies in very different (and possibly adjacent) areas. Thus, even if the FCC could identify adequate available capacity, it would still be unwise to force all public safety agencies into a single band.

D. Configurability and Flexibility

The ability of public safety networks to provide one-to-many communications (think “calling all cars”) is essential to their effectiveness. Moreover, it is important that such networks be flexible and configurable so that they can include other groups (say, utilities when damage to an electric grid is involved) on an as-needed basis. In some cases, both of these features—i.e., a one-to-many functionality and an ability to create ad hoc networks of users—were lacking in traditional commercial networks. Increasingly, however, modern commercial networks (which are often software-based and designed for multiple applications) can support applications specialized for first responders, including sophisticated push-to-talk features.

²⁰ *The Development of Operational, Technical, and Spectrum Requirements For Meeting Federal, State, and Local Public Safety Agency Communication Requirements Through the Year 2010*, First Report and Order, 14 FCC Rcd 152 (1998); *Reallocation of Television Channels 60-69, the 746-806 MHz Band*, Report and Order, 12 FCC Rcd 22,953 (1997); Balanced Budget Act of 1997, Pub. L. No. 105-33, § 3004, 111 Stat. 251 (1997) (codified at 47 U.S.C. § 337(a)(1)).

²¹ *Why Can't We Talk*, *supra*, at 53.

E. Security

For public safety agencies, protecting the privacy of communications and guarding against malicious attacks on their communications services are critical priorities. To keep information private and guard against attacks, secure communications systems must encrypt communications (so that unauthorized users are not able to intercept them) and bilaterally authenticate both remote users and servers (to limit who has access to the system). In an ideal system, encryption keys can be dynamically assigned from a central management system so that additional users can be added as needed. Again, traditional commercial networks tend to lack sophisticated encryption and authentication capabilities. Going forward, commercial systems, such as the system MSV is developing for its ATC network, will increasingly deploy more sophisticated security features—such as Public Key Infrastructure (PKI)—and allow for applications that can provide additional security (e.g., through the use of stronger encryption, such as NSA Type-I).

III. MSV's Existing Satellite and Future ATC Services Provide Important Benefits to Public Safety Agencies

In evaluating the communication needs of public safety agencies, policymakers should reject the calls for a “one-size fits all” solution and recognize, as the Federal Wireless Policy Committee has put it, that “more than one service may be required to support” a next generation public safety network.²² In particular, policymakers should promote a hybrid approach that would incorporate LMR systems along with terrestrial, satellite, and emerging wireless broadband systems. Such solutions are only beginning to be tested, but it is increasingly apparent that traditional LMR systems can be provided along with ancillary terrestrial component satellite handsets that automatically switch between cellular and satellite systems (depending on which is available). Moreover, by designing such systems in a modular fashion, they can rely on

²² Federal Wireless Policy Committee, *Federal Functional Requirements for Commercial Wireless Services* (Dec. 11, 2001) (http://www.fwuf.gov/docs/rev_dec01.pdf); see also James Careless, *Speak Easy: Technologies To Improve Two-Way Communications for First Responders*, FRONTLINE FIRST RESPONDER (June 2003) (<http://www.msvlp.com/pr/pdf/speakeasyarticle.pdf>) (highlighting virtues of a multi-mode solution); Michael McShea & Richard Davis, *A Hybrid Approach*, MISSION CRITICAL COMMUNICATIONS 57 (April 2005); Alan Shark, *Don't Rule Out Either Option*, MISSION CRITICAL COMMUNICATIONS 60 (April 2005) (“no one system can or should meet all jurisdictional mission-critical needs”).

wireless broadband networks, such as those using WiFi technology as well as still emerging technologies (like the next generation WiMAX standard). Notably, a WiFi-like system, like satellite technology itself, is relatively robust and, as demonstrated in the aftermath of Katrina, can be important in assisting the communications needs of public safety agencies.²³

One important reason for relying on commercial systems in general and hybrid satellite-terrestrial systems in particular is that they enable public safety agencies to benefit from the considerable economies of scale and enhanced functionalities that commercial providers can offer. Even under the very best of circumstances, public safety agencies are generally not able to build up the economies of scale and develop the network efficiencies of their commercial brethren. (This explains, in considerable part, why public safety equipment is generally quite expensive.) At a minimum, then, public safety agencies should take advantage of the favorable economics of commercial systems and expand their use of “off the shelf” services and products for at least some of their communications needs. As we explain below, MSV’s satellite services in general and its hybrid satellite-terrestrial offering in particular meet the requirements outlined above and are well suited to be a valuable component of public safety wireless systems.²⁴

To supplement traditional terrestrial networks, it is critical to incorporate satellite services into public safety wireless systems. First, as Katrina made clear, satellite systems are the best means of ensuring that public safety communication systems remain operational during dire circumstances. Second, as the case of the New Mexico State Police demonstrates, satellite technology can assure complete coverage to public safety agencies. In particular, the New Mexico State Police Department has compensated for the lack of ubiquitous coverage and ability to carry data on its private LMR by contracting with MSV for access to a satellite-based solution that provides ubiquitous coverage, reliable push-to-talk services, and access to data communications capabilities.

²³ Kenneth Moran, Presentation at the Agenda Meeting of the Federal Communications Commission (September 15, 2005); see also Clive Thompson, Talking In The Dark, N.Y. Times Magazine 24 (September 18, 2005) (discussing how Wi-Fi-like systems using mesh technology can provide reliance and redundant communication networks).

²⁴ MSV is the leading developer of ATC systems, with 800 different covered claims in its 6 patents received to date and 70 additional patents pending. See Press Release, Sixth Comprehensive Patent Issued to Mobile Satellite Ventures (May 18, 2005) (http://www.msvlp.com/pr/news_releases_view.cfm?id=62).

Finally, with the FCC approved ATC architecture that MSV will begin rolling out for its hybrid satellite-terrestrial system, the price of the service will be substantially less than current satellite systems. By using mainstream devices as well as more efficient terrestrial systems where appropriate, a hybrid satellite-terrestrial system provides significant cost savings *vis-à-vis* traditional satellite systems and will be available at reasonable prices from the launch of the product. More fundamentally, by using a terrestrial component, such systems can build up significant economies of scale that drive down the overall cost of the relevant equipment, meaning that the price of this service will decline dramatically as subscribers adopt it and the network enjoys greater scale economies. Significantly, even as to one of the advertised strengths of private LMR systems *vis-à-vis* commercial networks—the ability to provide coverage wherever it is needed—hybrid satellite-terrestrial systems can provide the best of both the commercial model as well as the traditional LMR systems. Thus, for carriers looking at the expense of adopting new LMR systems for remote areas and the ongoing costs of maintaining the necessary equipment, a hybrid satellite-terrestrial system provides an exciting alternative.

MSV's network provides a reliable and flexible wireless communications product that will become even more attractive once its ATC service is deployed. Unlike most commercial networks, hybrid satellite-terrestrial systems can be used when the local power grid fails or, in a situation like Katrina, when the available terrestrial networks are inoperable. In particular, hybrid satellite-terrestrial handsets can switch seamlessly and instantaneously between cellular networks (when a base station is operating nearby) and a satellite network (when there are no base stations in the area). In terms of providing priority access, MSV is designing its system so that, in the case of emergency events, the public safety operators can enjoy priority access to the extent necessary to preserve public safety communications. To do so, MSV is incorporating priority-precedence features contained within today's 3 G (and some 2 G) cellular standards.²⁵ Moreover, with its satellite network, MSV can provide superior call completion rates—even for calls that require coast-to-coast connectivity—when delivering “on network” calls that eliminate (or, in some cases, limit) any dependency on the external wireline network.

²⁵ The essence of priority and precedence features contained in, or under development for, 3G cellular standards, is that they enable pre-defined user classes to obtain priority access to wireless communications resources. Consider, for example, the enhanced Multi-Level Precedence and Preemption (eMLPP) feature within the Global System for Mobile Communications (GSM) air-interface, which provides for up to five distinct priority classes that (during periods of congestion) allow an “emergency call” to queue for the next available radio channel.

In terms of flexibility and configurability, MSV's hybrid satellite-terrestrial system will allow for the creation of ad hoc user groups of 2 to 10,000 that can use push-to-talk functionality and communicate among an interdisciplinary team through a large group dispatch service. Significantly, MSV expects the set-up time for such push-to-talk functionality to be similar to its existing offering, with a range of 1.5-2.0 seconds for talk group initiation and a delay between speakers of about 0.5-0.75 seconds. To be sure, this system may not be appropriate for "shoot-don't-shoot" situations, but should be adequate for an array of scenarios where push-to-talk systems are used by public safety agencies, including nearly all of the first responder communications needs in the wake of Katrina.

Increasing their reliance on commercial systems such as MSV's hybrid satellite-terrestrial system does not mean that public safety agencies should abandon their existing LMR systems. Rather, today's LMR systems often serve a very useful purpose and should be an important part of a hybrid network architecture. Along these very lines, both mission critical networks and critical infrastructure companies (such as utilities like the Tennessee Valley Authority) have begun to gravitate away from relying solely on their private networks. In particular, a number of entities that previously relied solely on their LMRs have concluded that they should continue to maintain such networks, but rather than upgrade them, they can increase productivity and cut costs by moving towards an integrated architecture that includes commercial wireless networks.

In terms of developing an optimal network architecture, public safety agencies should also be open to taking advantage of advances in wireless broadband technology developed for unlicensed spectrum. A public safety network might use, for example, current wireless local area network (WLAN) technology (i.e., the 802.11 (WiFi) standard) and, eventually, next generation systems (e.g., 802.16 (WiMAX) systems). To foster the adoption of such systems by local governments, the FCC recently made available access to spectrum in the 4.9 GHz band. As the FCC stated in its press release, "public safety licensees [can now] use a single, low-cost device to access the 4.9 GHz band, the U-NII band, and the ITS band, allowing them to enjoy savings that are typically limited to the high-volume commercial market."²⁶ Recognizing this opportunity, some police departments, like that of Salida, Colorado, have adopted solutions based

²⁶ News Release, FCC Improves Public Safety Access To The Latest Broadband Technology (November 9, 2004) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254117A1.doc).

on this technology, saving money and making police officers more productive in the process.²⁷ One means of providing wireless broadband service is to use ad hoc mesh networking systems. At present, such systems are still in their early stages, but they promise (as one vendor put it) “infrastructure-free, automatically established and maintained, and agile” network architectures.²⁸ The promised effectiveness of such systems, which rely on a different architecture from today’s established wireless technologies, reflects their ability to “forward data one hop at a time over a distributed network of autonomous nodes using new and more reliable and efficient schemes.”²⁹ To limit the need for a widespread deployment of devices with the embedded ability to re-transmit communications (i.e., routers), some cities have deployed systems with transmitters placed on existing infrastructure (like streetlamps) and with intelligent access points to connect to wired infrastructure at particular points. In Garland, Texas, for example, the local law enforcement agency decided to rely on such a network, concluding (after an experimental use of the technology on a limited basis) that installing access points and wireless routers on existing infrastructure would be cheaper than building new transmission towers for either cellular or private LMR transmissions towers.³⁰ Finally, mesh networking systems, which rely on the basic Internet suite of protocols, can be secured by installing firewalls and other security protections.

In short, an optimal public safety architecture would use a flexible system to accommodate different technologies. As depicted in Figure 1, a public safety agency can use a multi-mode device to access a hierarchy of wireless networks, beginning with a public safety LMR system at the center, then a commercial terrestrial network such as MSV’s ATC service and finally a satellite overlay.³¹ As noted above, public safety agencies might also choose to integrate a

²⁷ Jim Renton, *Notebooks and Wi-fi Keep Colorado Cops on the Beat*, MOBILE COMPUTING NEWS (March 8, 2004) (http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html?track=NL-315&ad=477866&Offer=t3.8).

²⁸ Michael Rauf & Eric Lefebvre, *Keeping the Wireless Connection Running*, 9-1-1 MAGAZINE 58 (Jan/Feb 2003) (http://www.novaroam.com/downloads/nr_911article.pdf)

²⁹ Rick Merritt, *Darpa Looks Past Ethernet, IP Nets*, EE TIMES (April 26, 2004) (<http://www.eet.com/showArticle.jhtml?articleID=19200111>).

³⁰ Kris Middaugh, *No More Towers*, GOVERNMENT TECHNOLOGY (May 2004) (<http://www.govtech.net/magazine/story.php?id=90189>).

³¹ Hybrid satellite-terrestrial systems rely on a satellite system that uses the same band of spectrum for an integrated terrestrial system. With such a system, MSV will achieve important spectrum efficiencies and economies of scale which will result in lower cost and more user-friendly consumer equipment than current MSS equipment. Such advancements are critical to deployment of MSV’s next generation system and will redound to the benefit of public safety agencies that adopt it.

terrestrial wireless broadband network. In any event, the core design principle is that networks should be extensible to other terrestrial networks in addition to the core commercial terrestrial and satellite components.

Both commercial and public safety-driven considerations explain why multi-mode networks are increasingly practical and appropriate. Consider, for example, that today's ordinary consumer wireless devices have two to four bands and at least some of tomorrow's devices will use WiFi networks where available (not to mention a GPS receiver, Bluetooth functionality, and even a receiver for specialized TV broadcasts). With an extensible network, the keys to integrating them together are (1) facilitating the back-end integration of the commercial network and one or more LMR systems; and (2) gradually adding new user devices that incorporate satellite connectivity, including push-to-talk. In principle, this integration can be accomplished by incorporating a second chipset that would enable the device to use a satellite-adapted version of a mass-market air interface (MMI) such as GPRS, CDMA, OFDM or WiMAX.³²

Based on current estimates, MSV believes that an OEM module incorporating the chipset necessary to enable a hybrid terrestrial-satellite system in addition to the local LMR would cost the public safety user between \$40 and \$80 per unit. While this is more than the additional cost of the consumer ATC product, it is substantially less than it would be without the economies of scale resulting from the consumer deployment of ATC. Notably, doing so is cheaper than investing in the software and equipment necessary to achieve interoperability solely by upgrading or replacing existing LMRs.³³ Moreover, achieving interoperability through a flexible architecture (i.e., one that can facilitate ad hoc user groups through shared terrestrial and satellite systems) can be done relatively quickly and cheaply (i.e., compared with SAFECOM's current projections for achieving interoperability³⁴)—at the same as providing critical redundancy benefits.

³² Meanwhile, the core radio would continue to have LMR, and could add other capabilities such as the IWIN 162 MHz.

³³ Chief Willis Carter, Statement to Senate Commerce Committee 9 (September 29, 2005) (<http://commerce.senate.gov/pdf/chiefcarter.pdf>) (estimating that improving existing radios to allow interoperability would cost \$800 per radio).

³⁴ The long term vision of SAFECOM foresees achieving interoperability by 2023. See David Boyd, Statement to the Senate Commerce Committee, Session on Communications Interoperability 2 (September 29, 2005) (<http://commerce.senate.gov/pdf/boyd.pdf>).

Ultimately, the network depicted in Figure 1 (on page 18) would include an overlay for public safety purposes. Significantly, the concept of such a virtual network could be implemented using the same capabilities that mobile virtual network operators (VNO)³⁵ use today. In order to ensure control, security, and availability, the core network would dedicate resources to the Public Safety VNO, which would operate the public safety serving-network based on applications and policies of its own choosing. The public safety agency would also have the option not only to integrate a multi-mode radio using physically separate modules, but ultimately to use software-defined radios to switch seamlessly between different networks and their associated functionalities.

The vision of using “smart radios” for public safety communications systems would, as Chairman Martin put it, enable them to use “multiple frequencies in multiple formats” and would facilitate a more “flexible infrastructure.”³⁶ As part of such a flexible infrastructure, Chairman Martin emphasized, public safety agencies would incorporate the use of satellite networks, as they “are, in some instances, the most effective means of communicating.”³⁷ Consequently, by using devices like that depicted in Figure 2, public safety agencies could benefit by using a combination of different networks and thereby enjoy (as Figure 1 reflects) a far more impressive footprint and greater level of redundancy than any individual system could offer on its own. Indeed, many public safety agencies recognize the need to incorporate multiple technologies into their system, but are looking for the leadership on what architecture to use as well as financial assistance to upgrade their systems.³⁸

³⁵ Mobile Virtual Network Operators (MVNOs) lack network infrastructure or licensed spectrum, but instead use another operator’s facilities and capacity to provide an alternative service. In a number of cases, they also possess the back-end systems and enhanced functionalities necessary to provide their service.

³⁶ Statement of Kevin J. Martin, Hearing on Communications in A Disaster 7 (September 22, 2005). Chairman Martin’s observation echoed the findings of an earlier GAO Report. That report explained that “[s]oftware-defined radios will allow interoperability among different agencies using different frequency bands, different operational modes (digital or analog), proprietary systems from different manufacturers, or different modulations (such as AM or FM).” Government Accountability Office, Protecting Structures and Improving Communications During Wildland Fires 61-62 (April 2005) (<http://www.gao.gov/new.items/d05380.pdf>).

³⁷ *Id.*

³⁸ Chief Willis Carter, Statement to Senate Commerce Committee 9 (September 29, 2005) (<http://commerce.senate.gov/pdf/chiefcarter.pdf>) (explaining that satellite technology must be a part of a solution that incorporates multiple approaches).

FIGURE 1

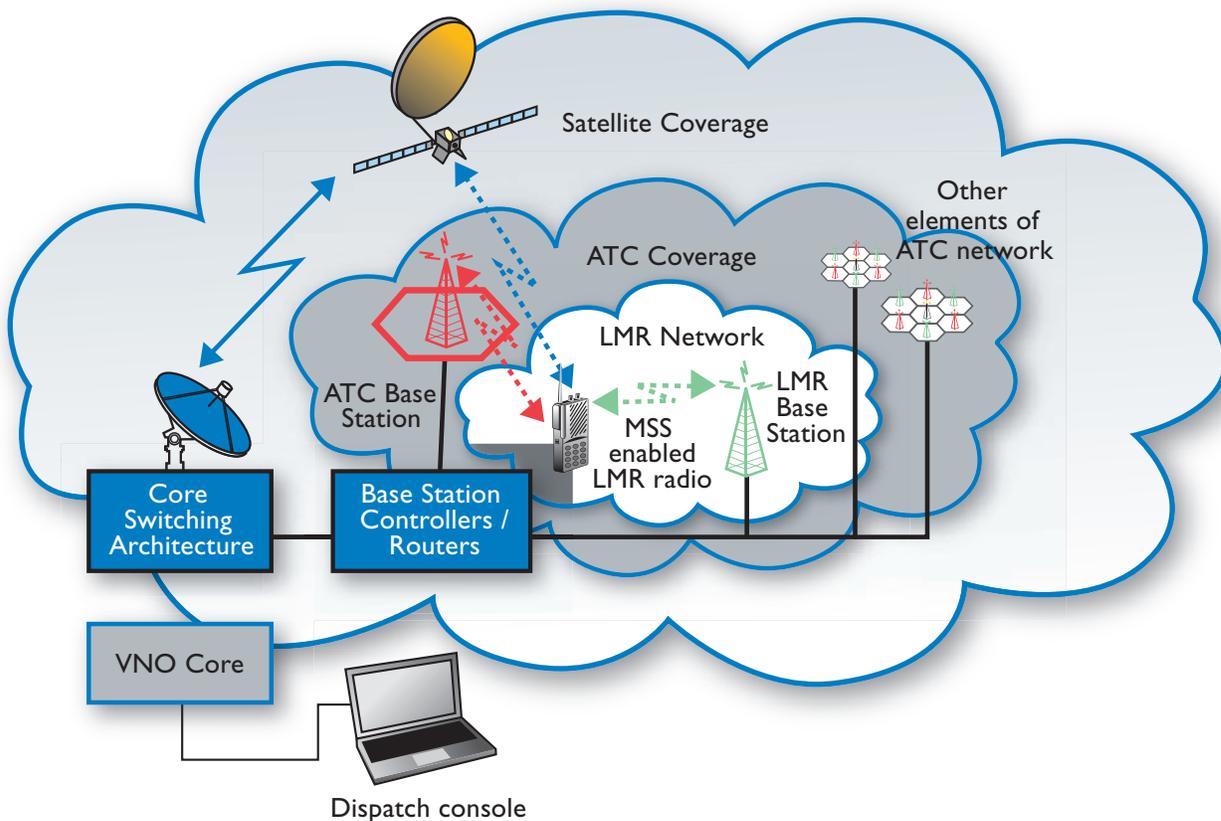
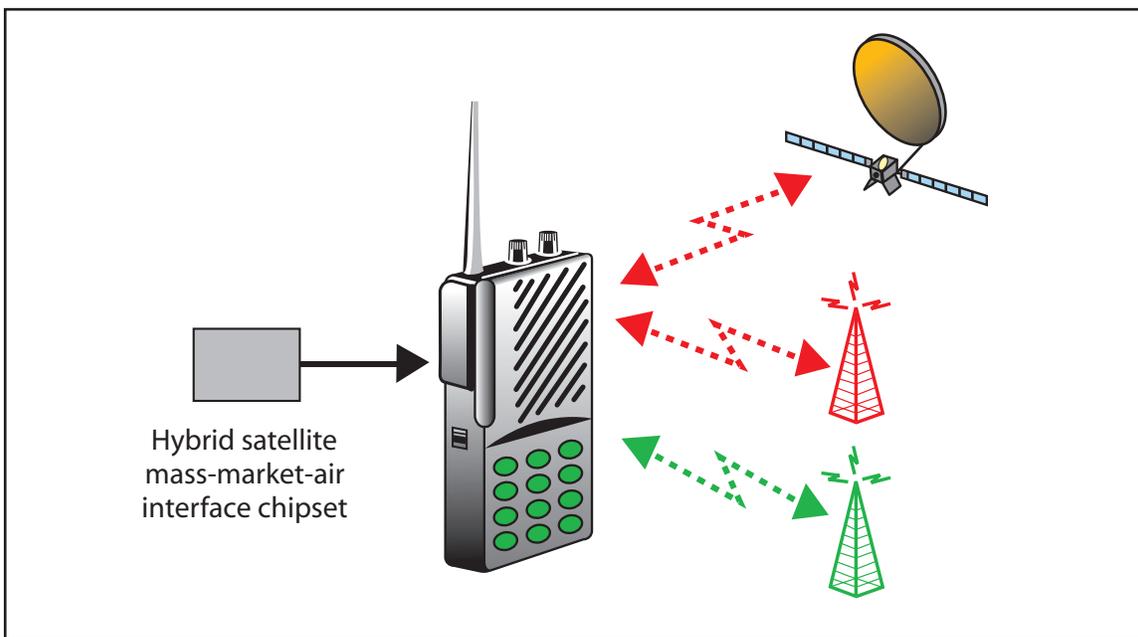


FIGURE 2



NOTE—Both diagrams are conceptual in nature and not drawn to scale

IV. A Policy Strategy For A Next Generation Public Safety Network

The federal government can play a very important role in facilitating the development of an interoperable broadband mobile communications network for public safety agencies. The best strategy, as suggested above, is not necessarily to promote next generation private LMR systems operated by local public safety agencies. Indeed, committing to such a limited vision might well prove problematic on a number of scores (e.g., locking in a costly and potentially inferior technology). Rather, the government should appreciate that the ideal mix between public and commercial networks is one it cannot divine in advance and it should thus promote a hybrid model of public safety networks such as that outlined above. To implement such an approach, we recommend three critical regulatory strategies: (A) making available additional spectrum that can be used for public safety applications by commercial providers; (B) recognizing that a policy of spectrum flexibility benefits public safety agencies by enabling commercial providers to meet their needs; and (C) ensuring that additional appropriations to aid the development of public safety communications promotes the flexible architecture described herein.

A. Making More Spectrum Available for Public Safety Purposes

For quite some time, the discussion over “making available additional spectrum for public safety agencies” has focused on dedicating spectrum for private LMR systems operated by specific agencies. Moreover, this discussion has often centered on the 1996 recommendation by the Public Safety Wireless Advisory Committee that 25 MHz of spectrum was needed by 2001 for public safety purposes, with an additional 72.5 MHz required by 2010. Notably, this recommendation assumes both that (1) achieving interoperability and providing mobile broadband capability will require more spectrum to be specifically dedicated to public safety providers; and that (2) the transition to digital television will be completed in a timely manner so as to free up spectrum for this purpose. Both propositions, however, are far from clear, thereby raising the question of what alternative strategy policymakers might use to enable public safety agencies to migrate toward a next generation network.

Many policymakers continue to take the traditional perspective of focusing on particular spectrum as designated for certain purposes. In the case of public safety, the historical use of spectrum in and around the 700 MHz band makes it understandable that policymakers would focus on whether additional spectrum in this band is necessary to facilitate the transition toward a next generation public safety communications system. But policymakers should be careful not to indulge the two assumptions questioned above—that providing specialized public safety spectrum is necessarily the best policy and that the digital transition will be completed in a manner that will make available such spectrum in a timely fashion. Rather than indulge such assumptions, we urge policymakers to think more broadly about what it means to make more spectrum available for public safety uses.

A broader perspective on the issue would appreciate that the Commission's recent action related to enabling public safety agencies to use spectrum in the 4.9 GHz band for wireless broadband is a form of making additional public safety spectrum available. Thinking even more broadly, it is clear that flexible policies related to SMR spectrum—including its decision to allow Nextel to accumulate dispatch licenses—promoted the development of public safety spectrum, as many public safety agencies now use Nextel's services and benefit from its economies of scale. Similarly, with respect to MSV, the Commission's policies authorizing the use of ATC—as well as its efforts now underway to finalize the distribution of surrendered MSS spectrum in the S Band—promise to make available spectrum that will be commercialized in a manner that will benefit public safety agencies.³⁹ In addition, in existing MSS bands, such as the L band, it is crucial that the relevant assignments be sensibly configured (e.g., contiguous so as to minimize the needs for guard bands and to support wide-band carriers) so as to ensure efficient use of spectrum and to facilitate broadband applications.

In short, policymakers should appreciate the importance of committing spectrum to commercial providers capable of offering service to public safety agencies. In the case of

³⁹ The Commission expressly recognized the public safety benefits of ATC in authorizing its use, concluding that “ATC may enhance the nation’s overall ability to maintain critical telecommunications infrastructure in times of crisis or disaster.” *Flexibility for Delivery of Communications by Mobile Satellite Service Providers in the 2GHz Band, the L-Band, and the 1.6/2.4 GHz Bands*, Report and Order, 18 FCC Rcd 1962, ¶ 29 (February 10, 2003).

satellite providers like MSV, it is not merely sufficient for the FCC to allocate spectrum for use by satellite providers, but it is also critical for it to provide certain and stable assignments of satellite spectrum. Only with such stable assignments, and the ability for providers to undertake significant investments over a period of time, will satellite providers be able to deploy innovative offerings like a hybrid satellite-terrestrial system that will ultimately benefit public safety agencies as well as other consumers.

B. A Policy of Spectrum Flexibility Benefits Public Safety Agencies

It is crucial that policymakers appreciate how promoting spectrum flexibility will greatly benefit public safety agencies. As the Spectrum Policy Task Force Working Group on Spectrum Rights and Responsibilities explained the vices of the old approach:

From the Commission's experience with command-and-control regulation, it is apparent that overregulation can deter both efficiency and innovation. The highly regulated nature of certain services has tended to discourage technological change because the means of providing permissible services are narrowly defined in terms of current and outdated technology. Moreover, in cases where licensees are limited in what services they are permitted to offer, they have no incentive to seek out a higher valued use for the spectrum.⁴⁰

The Commission's new perspective on spectrum policy takes a fairly critical perspective toward the classic "wise man" restrictions on how spectrum can be used and instead calls for "a light touch and a sense of humility" in developing rules that restrict uses of the spectrum.⁴¹ Thus, as the FCC's Spectrum Policy Task Force concluded, the Commission should look "to increase opportunities for technologically innovative and economically efficient spectrum use, spectrum policy must evolve toward more flexible and market-oriented regulatory models."⁴²

⁴⁰ Federal Communications Commission Spectrum Policy Task Force, *Report of the Spectrum Rights and Responsibilities Working Group 11* (November 15, 2002) (<http://www.fcc.gov/sptf/files/SRRWGFinalReport.pdf>).

⁴¹ Jonathan S. Adelstein, *New Frontiers in Wireless Policy: A Framework for Innovation 3* (April 9, 2003) (http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-233139A1.pdf).

⁴² Federal Communications Commission *Spectrum Policy Task Force, Spectrum Policy Task Force Report 3*, ET Docket No. 02-135 (November 15, 2002).

By reforming its traditional policy toward spectrum management, the Commission will, as Chairman Martin explained, move toward a model of “flexible allocations (that are technology and service-neutral)” of spectrum licenses.⁴³ This model, which the Commission has begun promoting through initiatives such as its Secondary Markets Order,⁴⁴ promises to “create strong incentives for making use of excess capacity” of spectrum already allocated in inflexible ways.⁴⁵ Significantly, by continuing to make progress on spectrum reform more generally, policymakers can assist public safety agencies in particular by helping to make the network architecture outlined above more effective and less expensive.

C. Funding For Public Safety Agencies Should Promote A Flexible Architecture

For many public safety agencies, their first priority and instinctive response is to replace their old equipment with expensive, often proprietary, and single-use systems. In many respects, public safety agencies’ attachment to LMRs of the kind that have served them relatively well is readily understandable—after all, familiarity often leads to comfort. In the case of technology products like mobile radios, however, public safety agencies should appreciate that (1) multi-mode radios; (2) economies of scale from off-the-shelf and commercially provided products; and (3) the opportunity to incorporate satellite backup into their systems are all opportunities that cannot be ignored. To facilitate greater understanding of such issues and to help develop the relevant technology, policymakers should consider funding both development of prototype models and demonstration projects as well as to fund greater research into the development and deployment of advanced technologies.

In providing important leadership on this issue, the federal and state governments should not allow local purchasing agents to act on auto-pilot and miss the option to migrate to a flexible,

⁴³ Kevin J. Martin, *U.S. Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (<http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html>).

⁴⁴ *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, Report and Order, 18 FCC Rcd 20,604 (2003).

⁴⁵ Kevin J. Martin, *U.S. Spectrum Policy: Convergence or Co-Existence?* (March 5, 2002) (<http://www.fcc.gov/Speeches/Martin/2002/spkjm202.html>).

next generation architecture. By using its power of purse thoughtfully, the federal government can play an incredible important role in this regard. Most important of all, policymakers should avoid requiring or creating incentives that would have the effect of foreclosing the type of architecture embraced by this White Paper.

CONCLUSION

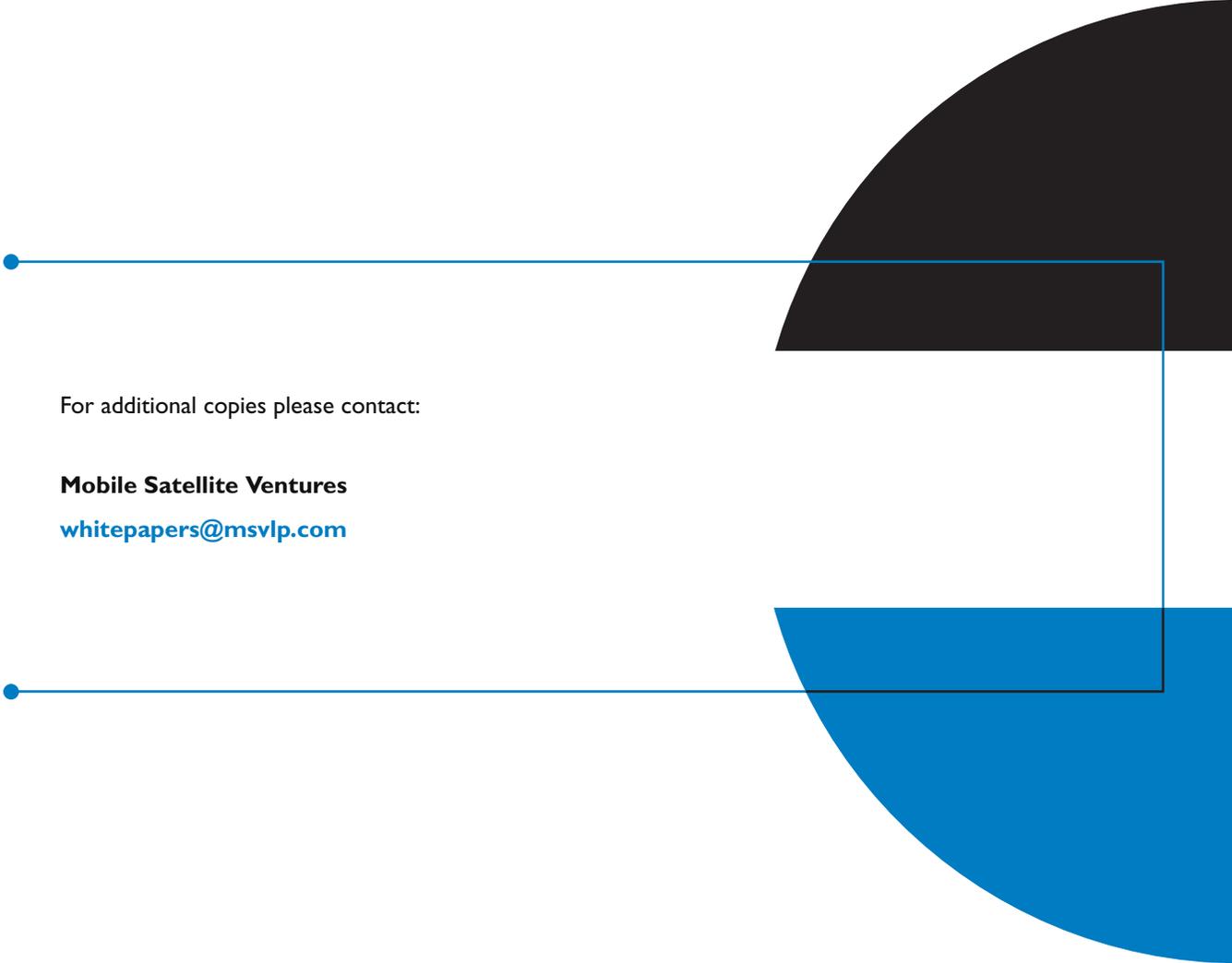
To learn from what went right and wrong in the aftermath of Hurricane Katrina, policymakers should avoid the impulse to assume that simply granting more spectrum for public safety agencies and appropriating more money to invest in LMRs will solve the problems of public safety communications. Rather, both policymakers and the public safety agencies themselves should look beyond this traditional mindset and develop a next generation architecture that would incorporate satellite, terrestrial, and emerging wireless broadband networks into a single seamless system. To promote this system, policymakers should focus on making spectrum *generally* available for broadband uses, whether via unlicensed WiFi-like systems, licensed commercial carriers, or satellite providers (including those using hybrid satellite-terrestrial networks with the aid of ATC technology) and ensuring that any government funding promotes a flexible architecture for public safety communications. By so doing, policymakers can best advance a next generation public safety communications strategy that can provide a reliable, survivable, and secure network for all first responders.

Particularly in light of the lessons underscored by Hurricane Katrina, adhering to the traditional model of relying solely on LMRs is no longer sustainable and policymakers must consider a more flexible and robust next generation architecture for public safety communications. Significantly, such a system would facilitate the greater use of satellite technology, such as was used effectively in New Orleans and the Gulf Coast in the wake of Katrina, and would embrace the use of hybrid satellite-terrestrial systems. In so doing, policymakers would make available far more cost-effective access to satellite technology than today's satellite terminals and ensure that users of this technology only used the satellite capacity when it is truly needed. And most importantly, such networks would switch seamlessly between available networks to enable first responders to use a single handset and not worry about what network is optimal; instead, the device would automatically select the appropriate network.

By implementing effective spectrum policies, encouraging the developing of hybrid solutions, and funding the purchase of more technically advanced solutions (e.g., multi-mode radios that include satellite and other technologies), policymakers can advance a next generation public safety network strategy. Notably, by promoting a public safety network where agencies can use spectrum licensed to commercial providers, available in unlicensed bands as well as dedicated to their private LMRs, public safety agencies will gain the benefits of a modern, innovation-rich, low cost network. In particular, public safety agencies will benefit from modular, extensible networks that can take advantage of cutting edge applications that ride on their private LMR, a commercially provided, or an unlicensed wireless broadband network. If, by contrast, policymakers focus exclusively on supporting single purpose LMR equipment and dedicated spectrum (say, in the 700 MHz band), they risk pursuing an antiquated technological architecture that will continue to leave public safety agencies without the best available tools for interoperable, reliable, secure, and broadband communications.

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 an Associate 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)."



For additional copies please contact:

Mobile Satellite Ventures
whitepapers@msvlp.com

EXHIBIT B

***The Impact of a Dual-Mode Mobile Terminal
on the Adoption of Wireless Broadband
by Public Safety Agencies***

***Charles L. Jackson
JTC, LLC***

***Coleman Bazelon
The Brattle Group***

Table of Contents

Introduction.....	3
The Economics of Sustainable Adoption.....	4
Ease of Innovation	6
Risk	8
Expected Profit.....	8
Individual Preferences and Circumstances	9
Economies of Scale.....	9
Summing Up	10
Public Safety Agency Needs.....	10
Counting Benefits	12
Conclusions.....	14
About the Authors.....	16

Introduction

The FCC has licensed 10 MHz of spectrum in the 700-MHz band (the “PS Band”) to the Public Safety Spectrum Trust (“PSST”) for a national, interoperable public safety broadband network. Eleven states, regions, and municipalities have asked the FCC for authority to begin deploying facilities in this band. The PSST has supported many of these requests. Aggressive plans for deploying commercial wireless services in other portions of the 700-MHz band are driving development of base station equipment that can be adapted for use in the adjacent PS Band. Thus, we expect that base station equipment will soon be available for deployment of public safety broadband services.

Handheld mobile broadband terminals designed and built for the special requirements of public safety agencies, including operation on the public safety broadband spectrum block (the “PS 700 Block”), are also essential elements of a robust, reliable public safety wireless broadband network. Development of such devices requires roughly two years and substantial commitments of capital. Unlike commercial frequency bands in which spectrum is licensed to well-capitalized commercial wireless carriers, no single large entity can guarantee widespread distribution and adoption of new devices for the PS Band. Without such devices, the most important capabilities of a public safety broadband network cannot be realized, and state and local government may be less likely to deploy public safety broadband networks until such devices are available. Therefore, we believe that accelerating development of public safety 700-MHz devices would accelerate the adoption of public safety broadband communications generally.

However, difficulty in financing the high cost of public safety broadband infrastructure means that the pace of deployment is likely to be uneven and uncertain. Furthermore, some regions cannot be served economically by terrestrial wireless infrastructure. Dual-mode terrestrial/satellite devices such as those that SkyTerra proposes to develop would make practical the deployment of 700-MHz terrestrial broadband infrastructure by public safety agencies located in areas of low population density. It would be uneconomic to

build infrastructure providing terrestrial coverage of more than a small fraction of the area served in these areas of low population density.¹

We estimate that almost 50,000 public safety personnel would be candidates for these devices in such areas, and more than 100,000 personnel would be candidates for these devices in areas where full-coverage terrestrial networks are not economic. The availability of dual-mode devices would also facilitate adoption of wireless broadband by public safety in every area of the nation by making the process of adopting wireless broadband easier. It would make adoption less costly for many agencies and less risky for all agencies. In this paper, we first consider the economic factors that affect adoption of innovation and consider how those factors could influence sustainable adoption of mobile broadband services by public safety agencies. We then use available data to estimate the number of people who live in areas where a dual-mode device would make broadband applications possible or areas where dual-mode devices would permit area-wide service. Using these population estimates, we derive estimates of the number of public safety personnel in these areas. Finally, we offer our conclusions.

The Economics of Sustainable Adoption

Mobile broadband services cannot be adopted by public safety agencies until all essential network elements are available, and mobile terminals are essential elements of a mobile

¹ SkyTerra has informed us that they are proposing development of two devices, one data-only handset and one voice-enabled handset (similar to a PDA). Current public safety land mobile radio systems are narrowband terrestrial systems optimized for voice. The data-only device fits the needs of agencies that wish to continue to use their existing system for voice communications and deploy an overlay network for broadband data. The dual-mode device meets the needs of agencies that wish to move all communications to an integrated broadband network. These devices will support broadband terrestrial communications using the LTE standard recently chosen by the public safety community. In normal circumstances, the satellite links will not provide “broadband” service as defined in the NOFA; however, they will be capable of supplying both “high-speed” services and “advanced” services according to recent FCC definitions. See FCC report, High Speed Services for Internet Access: Status as of June 30, 2008 (released July, 2009) (which uses the term *high-speed* to describe services that provide in excess of 200 kilobits per second (kbps) in at least one direction and the phrase *advanced services* for those providing transmission speeds in excess of 200 kilobits in each direction). Some applications, such as live, high-resolution video streaming, although technically feasible, may not be suitable for wide-scale use on satellite networks. However, satellites will provide advanced, two-way high-speed data links to handheld mobile terminals, and these links are highly capable of handling most or all other mobile data applications that would be routinely delivered over a public safety terrestrial broadband network.

broadband network. Development of such devices requires roughly two years and substantial commitments of capital. However, even when 700-MHz public safety devices are available, many agencies will be reluctant to deploy 700-MHz wireless broadband services until coverage extends across a large portion of the agencies' jurisdiction. Broadband user terminals that can communicate with both terrestrial base stations using the 700-MHz public safety bands and with satellites would substantially speed the adoption of broadband wireless by public safety agencies—particularly, public safety agencies operating in rural areas. If the dual-mode devices were the first public-safety oriented 700-MHz devices to become available, they would accelerate public safety broadband adoption throughout the nation.

There is a substantial literature on the adoption of innovations. Economists, sociologists, and marketing experts have researched adoption of innovations.² Gilbert and Rohlfs proposed a method of analyzing the new product adoption process that can be applied to understand the impact of a dual-mode terminal on broadband adoption by public safety.³ The Gilbert and Rohlfs analysis predicts the relative speed of adoption of an innovation on the basis of consideration of six demand-side drivers and six supply-side drivers. Those drivers are described in Table 1 and listed in order of importance.

² An early book on the topic was Everett Rodgers's *Diffusion of Innovations* first published in 1962. Marketing Professor Frank Bass's paper "A New Product Growth Model for Consumer Durables," published in 1969, offers a more quantitative model of the adoption of new products. Rohlfs's 1974 paper "A Theory of Interdependent Demand for a Communications Service" explores the relationship between network externalities and pricing in the adoption of network technologies. A recent survey focusing on telecommunications products is "Telecommunications Demand Forecasting—A Review," Robert Fildes and V. Kumar, *International Journal of Forecasting*, 18(4), October–December 2002, pp. 489–522

³ "Forecasting Technology Adoption with an Application to Telecommunications Bypass," Richard Gilbert and Jeffrey Rohlfs, in A. de Fontenay, M. H. Shugard and D. S. Sibley (Eds.), *Telecommunications Demand Modeling: An Integrated View*, North-Holland, Amsterdam, 1990, pp. 399–412.

Table 1.
Gilbert/Rohlfs Adoption Drivers

Demand Side	Supply Side
Expected Profit	Productive Capacity
Risk	Producer Reputation
Ease of Innovation	Industry Concentration and Ease of Entry
Capital Stock	Economies of Scale
Scale and Integration	Complementarities and Network Effects
Individual Preferences and Circumstances	Product Promotion and Price Competition

Designing and bringing to market a dual-mode terminal for public safety would have profound effects on the three most important demand-side factors—expected profit, risk, and ease of innovation. It would also affect the sixth demand driver—individual preferences and circumstances—and have some impact on one supply side driver—economies of scale. Below we consider each of these—albeit in an order chosen to improve exposition.

Ease of Innovation

A dual-mode terminal would make adoption of wireless broadband access by public safety far easier. First, the presence of the satellite mode means that an agency could experiment with new data-centric satellite and 700-MHz wireless broadband applications with much lower capital expenditures than otherwise. Rather than needing to spend tens or hundreds of millions of dollars to build out a complete network before being able to test broadband access, a public safety agency would be able to erect a few sites in the most heavily trafficked areas; deploy dual-mode terminals to a few users, say, all the field supervisory personnel in an agency or all the users assigned to one command region; and test the utility of applications delivered to and from the dual-mode devices with live traffic across a significantly larger geographic area than would be possible with just the terrestrial infrastructure. Second, the availability of terminals with a satellite mode would permit an agency to use simpler, consistent procedures throughout its service region. Without the satellite mode, an agency would have to either (1) develop procedures that could cope with a user being outside the coverage area of the base station network or (2) not use wireless data access until terrestrial coverage was built out over the entire service

area. The first option is suboptimal because it would necessarily limit the usefulness of applications and functionality of the network (and therefore limits its cost-effectiveness). It also would require agencies to maintain legacy systems and operating protocols indefinitely, making it difficult or impossible to justify the new capital costs on the basis of long-term operating cost reductions. The second option is a significant economic and practical barrier to deployment of broadband services to public safety agencies.

Third, satellite-mode terminals would permit a public safety agency to begin using wireless broadband access applications as soon as the decision is made to deploy the capability, rather than waiting until the complete base station network is up and running. Given the lead time required for planning, capital budgeting, building permits, any necessary property acquisition, and other deployment activities, this would cut substantially the time required to get wireless broadband access operating for public safety, most particularly to those agencies most exposed to budgeting uncertainty. Moreover, with satellite mode devices available, public safety agencies and jurisdictions that cannot budget for a complete network build-out could build incrementally, using satellite services to fill in areas without coverage while terrestrial facilities are built, even if build-out takes many years.

Finally, the availability of satellite-mode terminals would ensure that most or all of the applications that agencies would come to rely on would be available in all circumstances and at nearly all times.⁴ The service provided by terrestrial networks is prone to disruption from a variety of unpredictable events (such as hurricanes and other natural disasters); in contrast, satellite service is interrupted only by significant, predictable blockages related to line-of-site issues (e.g., in-building). Because the satellite capability would be part of the access package available in standard, everyday devices, lack of familiarity with satellite communications would no longer prevent their effective use.

⁴ As described in footnote 1, satellite links provide performance capabilities that make them suitable for most or all mobile data applications that would be delivered over a terrestrial broadband network.

Risk

The availability of a satellite-mode option reduces many risks associated with public safety broadband deployments. Construction delays or delays in capital funding would not delay operational capability. Satellite-mode operation would provide a back-up option for failed base station sites. Satellite-mode operation also would provide a reliable communications link for units that had to operate outside the public safety agency's jurisdiction in unusual circumstances.

Further, making available a satellite access mode in a terrestrially oriented broadband wireless access device would guarantee that agency personnel would be familiar with satellite communications. This would ensure that the expense and time that would go into applications development and deployment over the broadband wireless access network would be leveraged in all circumstances, effectively making such applications available with far greater reliability than could be delivered over a single access mode device.

Expected Profit

Gilbert and Rohlfs, being economists, used the term *profit* to refer to the net benefits to the adopting entity. Public service agencies are not run for "profit" in the commercial sense; but, public safety agencies do consider the balance of costs and benefits in making procurement decisions. The more benefits delivered by an innovation in relation to its costs, the more likely that it will be adopted. The presence of a satellite-mode option would substantially lower the capital costs of jurisdiction-wide wireless access to broadband applications for many public safety agencies.

Consider the state of Nevada. The state consists of 17 counties with almost 70% of the population living in Clark County, which contains Las Vegas, and about 20% more living in Washoe County, which contains Reno. In contrast, 11 counties in Nevada have a population density of fewer than 10 persons per square mile. Lincoln County in southeastern Nevada has a land area slightly larger than that of Maryland but had a population of only 4,165 in the 2000 census. Public safety agencies serving Lincoln County cannot afford to build extensive terrestrial broadband wireless coverage over their entire jurisdiction. The satellite mode would give these agencies an affordable option to

extend the critical public safety applications that they use over their terrestrial wireless broadband network throughout their service area. A satellite-mode option would make a tremendous change in the balance of costs and benefits for such agencies.

Similarly, a satellite mode is the only way that statewide public safety agencies such as the Nevada Highway Patrol can have access to the key applications enjoyed over their limited terrestrial broadband wireless access networks when in Lincoln County and in other similar sparsely populated counties. For many agencies, the satellite-mode option is necessary to make pervasive availability of such applications affordable.

Individual Preferences and Circumstances

As described above, the new technologies that enable the inclusion of satellite air interface protocols and satellite RF capability into standard terrestrial broadband devices have significant benefits for those public safety agencies least likely to enjoy broad geographic benefit from terrestrial wireless broadband deployments. Absent a satellite option, these neglected groups might, in many cases, be forced to choose between coverage extension for their existing narrowband applications and the limited availability of broadband, with no additional coverage to more remote and therefore at-risk areas. The inclusion of a satellite mode in public-safety-oriented broadband devices would dramatically increase the utility of the basic suite of applications delivered over the terrestrial broadband wireless access network. It would ensure that public safety agencies would have the flexibility to choose both broadband and the superior coverage and survivability that only satellite can provide.

Economies of Scale

Development of dual-mode devices would influence one factor on the production side that would affect adoption, namely, economies of scale. Economies of scale are enjoyed when increases in production reduce the unit costs of production. In developing dual-mode devices, a manufacturer must overcome barriers to production related to design and initial production runs. In the absence of demonstrated market demand, which is unlikely to be apparent until terrestrial public safety broadband networks are widely deployed, it is unlikely that a manufacturer would invest the significant resources required to offer such devices to public safety agencies. By guaranteeing the initial production of dual-mode

devices (which may also be the first 700-MHz public safety devices to become available), the current grant application would ensure that these initial barriers are overcome. This would move a manufacturer down the cost curve, allowing devices to be produced more inexpensively, which, in turn, would speed the adoption of wireless broadband services by public safety agencies.

Summing Up

Giving public safety agencies the option of using dual-mode terminals would substantially speed the adoption of wireless broadband applications by public safety agencies. It would make adoption of wireless broadband easier by facilitating experimentation, by making operations simpler, and by permitting universal operation before terrestrial build-out is complete. It would also mitigate risks from network failures and construction delays. And, for many agencies, it would make the broad use of wireless broadband applications affordable when they would otherwise be prohibitively expensive. It would give all agencies a cost-effective option for service in rural areas.

Public Safety Agency Needs

As the above discussion shows, a dual-mode terminal would provide different benefits to different categories of public safety users. One particularly important dimension is population density. Consequently, we categorized public safety service regions by density in order to better understand how the benefits of a dual-mode terminal would be distributed. Specifically, we considered the regions served by public safety answering points (PSAPs). PSAPs are the call centers that take calls to 911. The nation is divided in nonoverlapping regions—each served by one of the approximately 6,907 different PSAPs.⁵

⁵ According to FCC, there are a total of 8,237 PSAPs. 709 of them are no longer considered a primary call taking answering point and 605 of them are secondary PSAPs associated with a primary PSAP. Another 16 PSAPs have been excluded due to data inavailability. This leaves 6,907 primary PSAPs used for the purposes of this analysis.

Table 2 shows the distribution of PSAPs by population density.⁶ The table also shows how many PSAPs have less than a given density and what the population of those PSAPs is. We found that about 4 million people live in the almost 700 PSAP regions with estimated population density of less than or equal to 10 pops/sq mi and that about 15 million people are living in PSAPs with less than or equal to 30 pops/sq mi.

Table 2.
Distribution of PSAPs by Population Density

Range of Population Density per Square Mile		Number of PSAPs in Range	Cumulative Number of PSAPs	Cumulative % of PSAPs	Cumulative Population
From	To				
0	1	86	86	1.25%	154,757.00
1	2	86	172	2.49%	529,738.00
2	3	75	247	3.58%	912,083.00
3	4	105	352	5.10%	1,443,475.00
4	5	79	431	6.24%	1,912,614.00
5	10	261	692	10.02%	4,180,804.00
10	20	430	1,122	16.24%	9,363,465.00
20	30	427	1,549	22.43%	15,545,718.00
30	40	438	1,987	28.77%	23,144,135.00
40	50	309	2,296	33.24%	29,936,439.00
50	100	1,029	3,325	48.14%	59,204,735.00
100	200	715	4,040	58.49%	88,935,985.00
200	300	398	4,438	64.25%	111,419,353.00
300	400	348	4,786	69.29%	129,558,137.00
400	500	247	5,033	72.87%	142,096,809.00
500	1,000	548	5,581	80.80%	177,611,148.00
1,000	2,000	740	6,321	91.52%	225,252,094.00
2,000	3,000	218	6,539	94.67%	244,655,091.00
3,000	4,000	183	6,722	97.32%	254,965,745.00
4,000	5,000	8	6,730	97.44%	256,579,741.00
5,000	>5,000	177	6,907	100.00%	270,292,054.00

Sources and notes:

This table is based on data from the 2000 Census, so the total reflects the population in 2000, not the current population.

⁶ In this analysis, we used the population density in the county where the PSAP is located as a surrogate for the population density in the PSAP serving area. We believe that for the purposes of this analysis, any errors introduced by this approximation are largely offsetting and not material.

Table 3 uses these population-density figures to divide the PSAPs into broad categories and shows what we judge to be the primary benefit of a dual-mode terminal for each category.

**Table 3.
Benefits of Dual-Band Terminal by Category of PSAPs**

PSAP Population Density (Population per square mile)	Primary Benefit	Number of PSAPs	% of All PSAPs	Population	% of Population
Less than 20	Essential for any significant coverage in the service area.	1,122	16.24%	9,363,465	3.46%
20 to 50	Essential for complete coverage in the service area.	1,174	17.00%	20,572,974	7.61%
50 to 500	Provides coverage in low-density regions of service area that would be expensive to build out.	2,737	39.63%	112,160,370	41.50%
More than 500	Provides a backup capability for downed towers, downed backhaul, power failures, and areas without coverage.	1,874	27.13%	128,195,245	47.43%
TOTAL:		6,907		270,292,054	

Counting Benefits

PSAP serving area boundaries usually fall along political jurisdictions. Thus, to a first approximation one might conclude that each PSAP corresponds to one fire department, one police department, and one EMS provider. However, this approximation is limited. Some public safety agencies such as the State Patrol or Natural Resources Police serve many PSAP regions. Some PSAPs cover the service regions of multiple police or fire departments. There are approximately 60,000 public safety agencies in the United States—three per PSAP would only account for 20,721 of them.

Table 4 reports the number of public safety agencies and field personnel.

Table 4.
Characteristics of Public Safety Agencies

Type of Agency	Number of Agencies	Personnel
Fire Departments	28,495	361,000
EMS Departments	5,841	201,000
Law Enforcement	27,496	861,000
TOTAL:	61,832	1,423,000

Sources and notes:

The number of agencies was obtained from SAFECOM, the Department of Homeland Security.

The number of personnel was obtained from the U.S. Bureau of Labor Statistics.

If we assume that the number of public safety personnel in an area is proportional to the population of that area, then we can estimate the number of public safety personnel for each population density category. Although the relationship between population and public safety personnel is unlikely to be strictly linear, we do not have enough information to estimate the relationship precisely. Errors could go either way. An area with low population density may have more than the average number of public safety personnel given that personnel are not divisible and a minimum of one is required. If population is sufficiently small, however, the actual number of personnel may be zero. The results of our calculations assuming a linear relationship between population and public safety personnel are reported in Table 5.

Table 5.
Estimated Public Safety Personnel by Category of PSAP Region

PSAP Population Density (Population per square mile)	% of Population	Fire	EMS	Law Enforcement	Total
Less than 20	3.46%	12,506	6,963	29,827	49,296
20 to 50	7.61%	27,477	15,299	65,534	108,310
50 to 500	41.50%	149,801	83,407	357,280	590,488
More than 500	47.43%	171,217	95,331	408,359	674,906
TOTAL:		361,000	201,000	861,000	1,423,000

To calculate the number of broadband devices for each agency, we need to estimate the number of devices that would be required to supply the agencies in each category. We believe that each law enforcement officer would benefit from access to broadband applications. It is less clear to us whether individual EMS technicians or paramedics would need a broadband terminal or whether a single broadband terminal in the vehicle would be appropriate. If an agency were to move to an integrated broadband network for all applications including voice, then a terminal per individual in the field would be appropriate. But even if an agency did not do so, if broadband applications became widely used for administrative and managerial tasks, it would become appropriate to provide all field personnel with broadband terminals. Furthermore, agencies would keep some inventory of back-up and spare devices, somewhat offsetting any field personnel who did not carry a device. Thus, in what follows, we define the population of interest as all public safety field personnel. However, the reader should keep in mind that under some scenarios, the number of devices needed could be smaller.

Using the data in Table 5, we deduce that there are almost 50,000 public safety field personnel for which broadband applications are essentially not feasible without dual-mode devices.⁷ More than 100,000 public safety personnel serve in regions where it is probably not economically feasible to build out complete terrestrial broadband coverage. Finally, there are about 1.3 million public safety personnel for whom a dual-mode device would provide valuable backup options and would make terrestrial build out more affordable.

Conclusions

A dual-mode device would speed broadband adoption by public safety agencies by facilitating experimentation, by making operations simpler, and by permitting universal operation before terrestrial build-out is complete. Risks would be reduced and affordability improved. For almost 50,000 public safety personnel serving about 10 million people, a dual-mode device would make broadband applications possible. For

⁷ Strictly speaking, these 50,000 could be served with a satellite-only option. However, such an option would sacrifice economies of scale in terminal production and would prevent agencies from installing terrestrial base stations in areas such as towns.

more than 100,000 more first-responders, a dual-mode device would make coverage throughout the service area possible. Dual-mode devices could provide substantial benefits to the great majority of the nation's 60,000 public safety agencies and could be a major factor in stimulating permanent adoption of mobile broadband by thousands of agencies.

About the Authors

Dr. Coleman Bazon

Dr. Bazon is an expert in regulation and strategy in the wireless, wireline, and video sectors. He has consulted and testified on behalf of clients in numerous telecommunications matters, ranging from wireless license auctions, spectrum management, and competition policy to patent infringement, wireless reselling, and broadband deployment.

Dr. Bazon frequently advises regulatory and legislative bodies, including the U.S. Federal Communications Commission and the U.S. Congress. He also has expertise in the federal government's use of discount rates for policy and regulatory analysis, intellectual property valuation, and antitrust and damages analysis.

Prior to joining Brattle, Dr. Bazon was a vice president with Analysis Group, an economic and strategy consulting firm. During that time, he expanded the firm's telecommunications practice area. He also served as a principal analyst in the Microeconomic and Financial Studies Division of the Congressional Budget Office where he researched reforms of radio spectrum management, estimated the budgetary and private sector impacts of spectrum-related legislative proposals, and advised on auction design and privatization issues for all research at the CBO.

Dr. Charles L. Jackson

Dr. Charles L. Jackson is an electrical engineer who has worked extensively in communications and wireless. He has been both a digital designer and a system programmer. He works as a consultant and as an adjunct professor at George Washington University, where he has taught graduate courses on computer security, networking and the Internet, mobile communications, and wireless networks. Dr. Jackson consults on technology issues—primarily wireless and telecommunications. Dr. Jackson served three terms on the FCC's Technological Advisory Council. He previously worked at both the FCC and the House Commerce Committee. He holds two U.S. patents. Dr. Jackson received his PhD from MIT.