

# Clearing the Air: Convergence and the Safety Enterprise

Philip J. Weiser  
*Rapporteur*



THE ASPEN INSTITUTE

*Communications and Society Program*

Charles M. Firestone

Executive Director

Washington, DC

2006

*To purchase additional copies of this report, please contact:*

The Aspen Institute  
Publications Office  
P.O. Box 222  
109 Houghton Lab Lane  
Queenstown, Maryland 21658  
Phone: (410) 820-5326  
Fax: (410) 827-9174  
E-mail: [publications@aspeninstitute.org](mailto:publications@aspeninstitute.org)

*For all other inquiries, please contact:*

The Aspen Institute  
Communications and Society Program  
One Dupont Circle, NW  
Suite 700  
Washington, DC 20036  
Phone: (202) 736-5818  
Fax: (202) 467-0790

Charles M. Firestone  
*Executive Director*

Patricia K. Kelly  
*Assistant Director*

---

Copyright © 2006 by The Aspen Institute

**The Aspen Institute**  
One Dupont Circle, NW  
Suite 700  
Washington, DC 20036

Published in the United States of America in 2006  
by The Aspen Institute

All rights reserved

Printed in the United States of America

ISBN: 0-89843-458-0

06-018

1562CSP/06-BK

# Contents

<b>FOREWORD</b> , <i>Charles M. Firestone</i> .....	v
<b>EXECUTIVE SUMMARY</b> .....	ix
<b>CLEARING THE AIR:</b>	
<b>CONVERGENCE AND THE SAFETY ENTERPRISE</b> , <i>Philip J. Weiser</i> .....	1
I. Vision Statement.....	3
II. Challenges that Plague Public Safety and Technological Opportunities that Lie Ahead .....	7
A. <i>Limitations of Public Safety Communications Systems</i> .....	8
B. <i>Opportunities from an Integrated Communications Architecture</i> .....	9
C. <i>A New IP-Enabled Architecture</i> .....	14
III. Transforming Public Safety Communications.....	20
A. <i>The Centrality of Incentives</i> .....	22
B. <i>Toward Effective Allocation of Responsibility</i> .....	25
IV. Conclusion.....	34
<b>APPENDIX</b>	
Participants.....	43
About the Author .....	47
Selected Publications from the Aspen Institute Communications and Society Program .....	49
The Aspen Institute Communications and Society Program .....	55

*The reader should note that this report is written from the perspective of an informed observer at the conference. Unless attributed to a particular person, none of the comments or ideas in this report should be taken as embodying the views or carrying the endorsement of any specific participant at the conference.*

# Foreword

The crisis in emergency response communications is a long-standing problem that has recently become impossible to ignore. The aftermath of Hurricane Katrina, including at least 1,330 deaths and \$96 billion in property damage,<sup>1</sup> was a striking reminder of what can happen when communications break down during a disaster. Even more tragic was the loss of life in the World Trade Center on September 11, 2001, caused by the lack of interoperable communications among New York City first responders. These tragedies are visible examples of problems of operability and interoperability in the “safety enterprise” sector we face every day.

The sources of confusion are complex but obvious. The public safety community relies on antiquated equipment that largely uses narrow-band connections, often forfeiting the benefits new digital technologies have rendered in the private sector. The combination of custom-manufactured, single-purpose radio equipment and dedicated spectrum generates added expenses and frustrates cooperation and information sharing. Although integrated broadband solutions to common problems have emerged in the military and commercial sectors, such technological answers are lagging in the safety enterprise sector—the vast array of public agencies (e.g., fire, police), hospitals, shelters, food, transportation, information providers, and many other public and private organizations that respond to disasters and emergencies.

Moreover, commonly proposed solutions are unlikely to end this fragmentation. Many participants in the current policy debate call for even more expensive and specialized equipment and dedicated spec-

trum. Such a response, however, fails to provide the broad shift in the approach to communications that the emergency community needs.

In short, what new policies might break through this situation that the federal government is willing to pay billions of dollars to correct and citizens in every community expect to be solved? More particularly, what communications and spectrum policies are necessary and appropriate to move the safety community to more modern, integrated, and effective solutions?

To address these issues, the Aspen Institute Communications and Society Program devoted its spring 2006 meeting of the Aspen Institute Roundtable on Spectrum Policy (AIRS) to a dialogue among public safety officials; spectrum experts; and executives, specialists, and governmental leaders from the telecommunications, Internet, and information industries in which participants sought to define the problems plaguing today's public safety systems and envision an effective modern system for tomorrow. The Roundtable, "Clearing the Air: Convergence and the Safety Enterprise," met at the Aspen Institute Wye River Conference Center in Queenstown, Maryland, May 7-9, 2006.

Phil Weiser, Executive Director and Founder of the Silicon Flatirons Telecommunications Program at the University of Colorado, has distilled the discussion into a coherent description of emergency communications problems and realistic means for solving them. Beginning with a vision statement that sets forth a new model for public safety communications and integrated information management across the entire safety enterprise, this report goes on to describe both the challenges public safety agencies

currently face and the new architecture they should embrace. It ends with a series of recommendations on how to make this vision a reality.

To unify the broader safety community while addressing differing needs, conference participants recommended a “network of networks” system for emergency communications. A backbone network based on an Internet Protocol (IP) standard would allow all connected agencies to share information and services without depending on outside or vulnerable physical networks. Such an architecture could accommodate advances in wireless and wired technologies and thereby continue to improve public safety effectiveness in the future.

The rapid evolution of commercial technology also provides an economic opportunity for the safety enterprise. Adopting and adapting commercially produced equipment could generate significant economies of scale while making networks more dependable during crises. More generally, participants suggested that the emergency response community should focus more on finding the best means to achieving specific goals (for instance, increasing mobility or dependability) rather than being trapped by certain preconceived technologies.

The greatest barrier to this ideal integrated system is not technical but managerial. Corporations and the military have already developed and tested digital communications technologies that could, with some adaptations, prove invaluable to emergency response services. Although a handful of existing demonstration projects are revealing technology’s potential in the safety-enterprise sector, such progress is moot without effective governance ensuring that such advances are universally and uniformly adopted.

During the Roundtable, participants developed next steps and long-term goals for federal, state, and local governments. Providing incentives and assigning responsibility could simultaneously ease and hasten the transition to a new model for safety communications and information management. Local agencies can no longer function effectively in isolation. Only with cooperation and integration at all levels of government can emergency response systems serve the needs of the public.

### **Acknowledgments**

The Roundtable is made possible by the financial support of industry sponsors. We gratefully acknowledge and thank the following competing companies for their support: Access Spectrum, AT&T, Cingular Wireless, Cisco Systems, Comcast Corporation, Credit Suisse First Boston, Cyren Call, Intel Corporation, Lockheed Martin, Motorola, National Association of Broadcasters, QUALCOMM, Verizon Wireless, and the Walt Disney Company.

Our thanks go to Philip Weiser for his concise and insightful report on the Roundtable. We are particularly thankful to our participants (listed in an Appendix to this document) for their openness, constructive attitude, and willingness to grapple with the issues facing the telecommunications industry. Finally, we thank Mridulika Menon, senior project manager; Patricia Kelly, assistant director; and Kate Aishton, program coordinator—all of the Communications and Society Program—for working behind the scenes to bring the Roundtable and this report to fruition.

Charles M. Firestone  
Executive Director  
Communications and Society Program  
Washington, DC  
August 2006



# Executive Summary

The 2006 Aspen Institute Roundtable on Spectrum Policy (AIRS) on “Clearing the Air: Convergence and the Safety Enterprise” emphasized the significant opportunity that is available to the public safety community to embrace new information and communications technologies. The public safety community today relies on (1) antiquated equipment that (2) largely uses narrowband connections, (3) is manufactured solely for their needs, and (4) uses spectrum dedicated to them. In response to the current crisis of public safety communications, many observers advocate “more spectrum and more money” to address what is often referred to (in misleading terms) as the “public safety interoperability problem.” The real problem, however, is that the current trajectory—including much of the current policy debate—focuses too narrowly on public safety entities; too specifically on issues related to radio communications; and, more generally, on the wrong solutions.

The AIRS participants recommend a new strategy. In particular, the public safety community should migrate away from its traditional reliance on specialized equipment and embrace an integrated broadband infrastructure that will leverage technological innovations routinely being used in commercial sectors and the military. Notably, by recognizing the power of Internet Protocol (IP) technology—regularly used by large, medium, and small enterprises to enable their businesses to work effectively—public safety agencies can unite disparate users, adopt enhanced and secure applications that use open standards, and facilitate interoperability through a “network of networks” strategy. Policymakers can thereby ensure a more effective emergency response strategy and more reliable communications during times of crisis.

The “network of networks” vision for emergency management (including public safety agencies) can work in conjunction with traditional reliance on dedicated land mobile radio systems. This vision, however, will provide far greater functionality than the traditional system and facilitate interoperability and data exchange between different stakeholders. It will give rise to economies of scale that will enable public safety agencies to adopt innovative technologies in an affordable manner. This vision will not implement itself, however. It will be realized only if federal policymakers develop a series of incentives and provide the necessary guidance so that federal, state, and local officials all do their parts to transform the current state of public safety communications and information management. Only through state-centered (or region-centered) leadership will a disparate set of public safety agencies be able to cooperate and embrace a next-generation vision that will provide far greater levels of operability and interoperability.

This report proceeds in three parts. First, it outlines a vision statement that clearly sets forth a new model for public safety agencies’ use of information and communications technology. Second, it describes the basic challenges that currently confront public safety agencies and describes the new architecture they should embrace. Finally, it sets forth a series of recommended strategies (and action items)—including a suggested assignment of responsibilities to federal, state, and local officials—that will enable this vision to become a reality.

**CLEARING THE AIR:  
CONVERGENCE AND  
THE SAFETY ENTERPRISE**

*Philip J. Weiser*



# CLEARING THE AIR: CONVERGENCE AND THE SAFETY ENTERPRISE

## I. Vision Statement

Public safety agencies have the opportunity to embrace and migrate to an affordable, effective, and efficient system of information and communications technologies and away from the expensive, “silo”-based approach. To do so, we recommend an integrated vision that addresses transport needs (i.e., wired and wireless access); embraces the open standards used widely by corporate information technology (IT) departments (e.g., those associated with Internet Protocol [IP] networking); includes adoption of applications and devices that are tailored to serving the needs of public safety agencies; and develops a system of governance, policies, and protocols to ensure that information and communications technologies are used effectively and intelligently. The technology to achieve this vision is not novel. It is widely available in the commercial sector and is proliferating at a very rapid rate. Moreover, this technology can be tailored to meet the unique needs of public safety without too much difficulty. Bringing it to the public safety sector, however, will require federal, state, and regional leadership—in particular, a set of high-powered incentives that will change the prevailing silo-based



**These changes...  
call for a culture change  
that embraces a new  
model of governance and  
a new technological  
architecture.**

This report uses the term “public safety” to capture a broad range of entities involved in emergency response. In particular, this report emphasizes that opportunities to use information and communications technology effectively are not limited to traditional “first responders” (such as fire and police) but also extend to all agencies and organizations that are likely to respond to emergency situations (e.g., agencies concerned with transportation infrastructure, public health providers, electric utilities). Moreover, this report also takes a broad view of information and communications technology—including not simply the wired and wireless local networks but also technology associated with accessing and sharing critical information—even though the text does, as a shorthand, sometimes use the term “public safety communications.”

approach that is common in today's world of public safety communications. These changes are not simply about throwing more money and spectrum at the problem; they call for a culture change that embraces a new model of governance and a new technological architecture.

Given the significant amount of spectrum and federal grants about to become available, there is an opportunity for the federal and state governments, along with public safety agencies and the private sector, to create a new vision for the use of information and communications technology in emergency management. Notably, unless the federal and state governments reform the system of governance for public safety communications, they will fail to implement a new technological vision that will solve the widely recognized communications needs of public safety agencies. Moreover, the current system of granting each agency its own license for a narrow slice of spectrum for its own use will not be able to support the broadband connectivity that is increasingly essential for effective public safety communications. Unfortunately, many policymakers do not appreciate the technological opportunity available to public safety, nor that facilitating more effective uses of information and communications technologies will depend far more on coordination and governance than simply providing more spectrum and federal grants.

The new technological architecture we recommend is a flexible structure that is based on a "network of networks" concept. The public safety community faces a disparate array of needs, but all public safety agencies can be served effectively by next-generation systems that enable them to access reliable, redundant broadband networks (including wireless and wireline). Regardless of the access technologies used, all public safety agencies should rely on an IP backbone network that would connect them with other relevant stakeholders (e.g., public health officials). By embracing IP technology and a network of networks concept, public safety agen-

cies will be able to use a set of tools and shared services that are not tied to—and dependent on—particular physical networks. In so doing, public safety agencies will migrate from reliance on single-purpose, fragmented networks into an interconnected system that will provide far more effective emergency communications—encompassing E-911 calls, an emergency alert system, and communications with public safety agencies as well as other affected entities (e.g. public health agencies).

Within this network of networks, there should be available, on a shared basis, several specific applications to enable effective emergency response. The list of agencies and organizations connected to the network should be as inclusive as possible, encompassing not merely traditional first responders and all emergency agencies but also those that would link up to an emergency alert system and those providing critical infrastructure (e.g., electric utilities) or other private or public entities. Significantly, connection to the network would not equate to access to all information carried on the network; a system of rights management would be implemented to govern appropriate use and access to the network for voice, data, images, or video. Moreover, connection to the network would be managed on a priority basis so that certain agencies would be guaranteed access during times of an emergency and others (such as commercial or selected governmental agencies) might be given lower priority or denied access during emergency conditions.

The fundamental premise underlying a network-of-networks architecture is that it can accommodate legacy solutions and does not require a one-size-fits-all solution. To its great credit, this architecture welcomes and benefits from innovation in wireless technology (such as high speed, wide area third-generation wireless broadband technology already being deployed by commercial wireless carriers, mesh networking wireless broadband systems, hybrid satellite-terrestrial networks,

and software-defined radio). Similarly, it enables disparate technologies—such as satellites, commercial terrestrial systems, and traditional land mobile radio systems—to work together. Managed properly, this architecture will enable continuous technological improvements (such as the ability to use multi-mode radios and decision support software) to incorporate and support a variety of wired and wireless devices. Significantly, such an architecture can enable joint-use public safety/commercial networks so that public safety can be given priority when necessary while allowing private-sector uses that will substantively defray network infrastructure and ongoing modernization costs. In short, with the proper incentives and the confidence that comes with seeing new systems work, we believe that the public safety community will be able to escape the current silo-based environment and benefit greatly from available commercial networks and general purpose technology that can be adapted and geared toward their specific needs.

In the wake of recent system failings in public safety and governmental communications (e.g., Hurricane Katrina and September 11, 2001), there is a policy window for creative thinking and development of a new model for public safety communications. Consequently, we urge policy-makers to reconsider the current policy course—consisting of more money and more spectrum for public safety agencies—and to embrace the virtues of a new model. In short (and as elaborated in Part III of this report), this model would rest on the following four basic principles:

- Migration away from a single-purpose network composed purely of specialized equipment and toward a multi-purpose, flexible network of networks concept.
- An end to the culture of information silos and embrace of an ecosystem of shared access to a network based on Internet

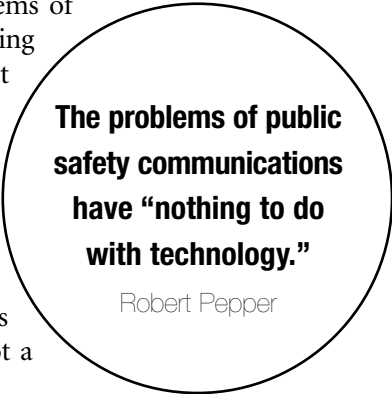


Protocol technology. By embracing such a unitary network for scores of different agencies, state governments can facilitate huge efficiency gains and provide more effective service to the public.

- Use of a rights management system that provides access to a variety of core services and valuable applications through a network of networks. This system can protect the integrity and security of sensitive government information and databases while enabling access—as needed and appropriate—across an array of agencies that will provide emergency services.
- An integrated system of leadership and governance to oversee the transition from from the balkanized system that limits the effectiveness of public safety communications to one based on a network of networks architecture.

## **II. Challenges that Plague Public Safety and Technological Opportunities that Lie Ahead.**

“The hard part” of solving the problems of public safety communications “has nothing to do with technology,” explained Robert Pepper, former Chief of the Federal Communications Commission’s (FCC) Office of Plans and Policy and Senior Managing Director, Global Advanced Technology Policy, Cisco Systems. Secretary of Homeland Security Michael Chertoff underscored this point recently as well, explaining that the challenge is “not a



**The problems of public safety communications have “nothing to do with technology.”**

Robert Pepper

technological challenge” but a management challenge.<sup>2</sup> Realizing that untapped technology is available to public safety is a critical part of any effort to address the limitations in public safety communications and information technology systems. Unfortunately, recent tragedies—notably, Hurricane Katrina and September 11—remind us that this insight must be addressed as a national priority.

#### *A. Limitations of Public Safety Communications Systems*

Hurricane Katrina did not *teach* us of any failings in public safety communications systems, said David Aylward, Director of COMCARE (a nonprofit organization that focuses on emergency communications); it merely reminded us of lessons that had been taught many times before.<sup>3</sup> These lessons, Pepper added, are that as a nation we must focus on three distinct concerns—operability, interoperability, and modernization. Operability addresses the point that public safety systems must be robust, reliable, and survivable. In the aftermath of Hurricane Katrina, the breakdown of conventional public safety systems—in particular, land mobile radio systems (LMRs)—as well as commercial systems (e.g., cellular and wireline services) left critical governmental services unable to function. In the case of the September 11 attack, by contrast, the inability of LMRs operated by different uniformed services—notably, police officers and firefighters—to interoperate (i.e., share information via voice and data communications on demand and in real time) prevented them from communicating with one another and sharing critical information.

The current path of public safety communications often involves use of specialized blocks of spectrum that are paired with single-purpose radio infrastructure. In practice, this arrangement means that public safety agencies are limited to narrowband channels and specialized

technology and do not benefit from economies of scale. Most current interoperability initiatives are limited by this legacy mindset—that is, they often revolve around efforts to dedicate more spectrum to public safety for the explicit purpose of promoting interoperability between disparate technologies rather than promoting the concept of internet-working. Consequently, they often envision (and call for) the purchase of single-purpose equipment specially designed for public safety rather than adoption of commercial technology built around the network-of-networks concept.

The balkanized state of the public safety information and communication technology system, with different agencies (even in the same jurisdiction) using different islands of technology, is a case study on how *not* to develop an IT enterprise. First, by purchasing expensive, single-purpose radio systems, most agencies adopt an architecture that does not allow for evolution and dynamism. Second, the specialized radios generally purchased by public safety agencies are not—contrary to the aspirations of the Project 25 effort<sup>4</sup>—produced by a large number of vendors and remain very expensive. Finally, the IT systems public safety agencies use generally rely on intelligence embedded in the physical radios—as opposed to in a logical layer (e.g., consisting of Internet Protocol-related standards) that is easily configurable and extensible—and are not generally able to carry both voice and data communications.

### *B. Opportunities from an Integrated Communications Architecture*

In all sectors other than public safety, the powerful trend in IT as well as in communications policy is away from a silo mentality. Increasingly, IT and communications equipment can take advantage of enormous advantages in digital processing power (i.e., Moore’s law), digital compression technology, and advantages in storage technology. These

forces, often grouped under the framework of the “digital broadband migration,” are reshaping almost all aspects of the telecommunications industry. In particular, these technological developments—in conjunction with open standards associated with the Internet Protocol (IP)—facilitate enormous innovation and enhanced functionalities for new communication platforms.

Users of information and telecommunications technologies have adopted new digital technologies at a rapid clip over the past five years.



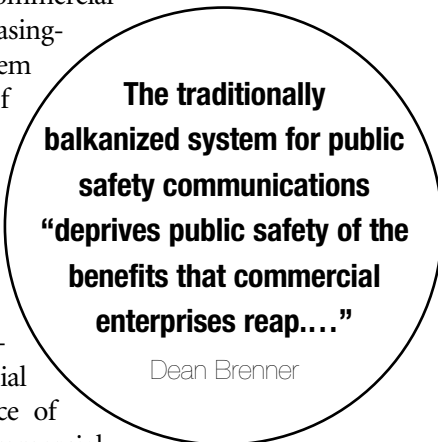
**“Emergency radio services need to exit their government technology ghetto and get onboard advanced networks—as smart customers, not Soviet-style suppliers.”**

Thomas Hazlett

Federal Express, for example, can track delivery of packages in a highly effective manner, using wireless technologies to provide information from a delivery agent back to its databases within seconds. Speaking from personal experience, Kevin Kahn, Intel Senior Fellow and Director of the Communications Technology Lab at the Intel Corporation, recounted that he has received a package and quickly accessed the FedEx website via his home computer to find it updated with the information that the package was delivered. Similarly, several AIRS conferees reported that the U.S. military has adopted IP technology that is enabling it to maintain its legacy technologies and adopt cutting-edge innovations.

Despite innovations associated with the digital broadband migration, public safety agencies continue to exist in a universe of specialized systems with a limited ability to adopt new technologies or interoperate with different systems. Thomas Hazlett, Professor of Law and Economics at

George Mason University (GMU), captured the roundtable’s perspective in stating, “Emergency radio services need to exit their government technology ghetto and get onboard advanced networks—as smart customers, not Soviet-style suppliers.”<sup>5</sup> Whereas public safety agencies once were regarded as “special” and unable to adopt commercial solutions, conventional wisdom increasingly recognizes that a balkanized system deprives public safety agencies of advanced technologies that can promote greater operability and interoperability.<sup>6</sup> As Dean Brenner, Vice President of Government Affairs for QUALCOMM, Inc., said, the traditionally balkanized system for public safety communications “deprives public safety of the benefits that commercial enterprises reap from the rapid pace of technological innovation in the commercial wireless market and the economies of scale that exist in that much larger market.” In practice, Brenner added, many public safety agencies use commercial wireless technology—such as wireless phones and personal digital assistants (PDAs)—but their use of that technology is not well coordinated, managed effectively for their needs, or coupled with adoption of appropriate applications.



**The traditionally  
balkanized system for public  
safety communications  
“deprives public safety of the  
benefits that commercial  
enterprises reap....”**

Dean Brenner

Charles Werner, Chief of the Charlottesville (Virginia) Fire Department, emphasized that public safety needs to “explore new paths and embrace new technology models.” To that end, Werner explained that Charlottesville is developing a demonstration project that will use an extensible, Internet-based architecture that will include commercial systems. This vision parallels that advanced by the National Reliability and

Interoperability Council's (NRI) Focus Group 1D, which calls for an emergency communications system that is linked in an "inter-network" fashion. In particular, the Focus Group's report recommended "a set of policies, tools, interfaces and standards that securely connect the multiplicity of local, regional and national wireline and wireless networks."<sup>7</sup>

Significantly, the new path made available by improved technology and being deployed in a few demonstration projects relies on a fundamentally different architecture than traditional public safety systems. This architecture, which is flexible, extensible, and based on IP technology, provides a far more effective means of ensuring both operability and interoperability than simply providing more spectrum and more funds for traditional equipment. As Jon Peha notes, "One cannot easily 'fix' interoperability as an afterthought to today's infrastructure, any more than one can easily 'fix' fuel efficiency on a racecar that was designed for maximum speed."<sup>8</sup> Moreover, fixing public safety's communications system, as Stagg Newman, President of Pisgah Communications Consulting and former FCC Chief Technologist, underscored, is not simply about technology; it's about effective governance systems that ensure that public safety agencies adopt appropriate technologies.

In the view of almost all roundtable attendees, public safety agencies should embrace the opportunity to purchase commercial, off-the-shelf products and services as part of a network-of-networks architecture. According to Kevin Kahn, there are huge economies of scale for equipment that uses the recently released spectrum in the 4.9 GHz band, and the soon-to-be released 700 MHz band for public safety uses will sit right near heavily used commercial bands. In short, Kahn added, there are "huge benefits by piggybacking on developments already happening in the \$35 radios being developed for the commercial bands." As Werner noted, public safety agencies "need to change the present para-

digm of what we are doing to get what we want,” focusing not on whether equipment is specially made for public safety agencies but on whether it meets the requirements and specifications for effective public safety communications.

Dale Hatfield, former FCC Chief Engineer and now adjunct professor at the University of Colorado, reminded the group that there are economies of specialization that, in some cases, outweigh the value of economies of scale. In particular, in certain parts of the country—Alaska and Montana, for example—there is a compelling reason to operate at 150 MHz, where radio propagation characteristics are more favorable for wide-open areas. Moreover, as Professor Hatfield explained, some of the specialized systems play a critical role in ensuring a very fast call setup time that is necessary for “shoot-don’t shoot situations.”

Specialized radios, as Hurricane Katrina reminded us, face major operability challenges during certain times of crisis, ranging from failure of communications-specific systems (antennas, transmitters) to nonspecific issues (electricity). In the case of Katrina, there was an absolute crisis of ability to communicate; the major source of viable communications technology was a satellite connection. Emphasizing this point, FCC Chairman Martin explained, “If we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications.” Moreover, in some areas, wireless Internet service providers (ISPs)—using more flexible emerging broadband systems—were able to restore service in a far more nimble fashion than specialized radios, deploying networks



**“If we learned anything from Hurricane Katrina, it is that we cannot rely solely on terrestrial communications.”**

FCC Chairman Martin

spanning several miles in just one to two days.<sup>10</sup> Finally, as Dean Brenner of QUALCOMM pointed out, portable equipment—such as very small deployable cellular base stations—can be used to provide service for emergency personnel within a given area when networks go down.

In short, even though there is no one-size-fits-all solution, there are tremendous improvements that can and must be made to our system of public safety communications through more effective coordination and a new architecture that is based on IP technology and a network-of-networks approach, tailored for the needs of public safety. This architecture need not and should not replace particular needs—for example, the decision to use satellite overlays in some cases and lower frequency bands in others. Instead, it should incorporate such options and displace the culture whereby local public safety agencies jealously safeguard their prerogatives and protect their turf. Only by changing that culture and adopting a network-of-networks architecture can public safety agencies upgrade their technological capabilities, facilitate more effective operability, and establish interoperable systems.

### *C. A New IP-Enabled Architecture*

In all major corporations there is a commitment to an enterprise architecture managed by an IT department. For public safety agencies, however, there is no such overall architecture and thus limited ability to connect networks and share information. Despite the success of the enterprise model, there remains a strong attachment to a “public safety exceptionalism” that calls for continued use of specialized radios and an interoperability solution that is based on interconnection at the physical layer. The AIRS conferees rejected this approach and recommend an IP-based solution for connecting disparate networks at higher layers (either the logical layer or the applications layer).<sup>11</sup> To appreciate the nature of this architecture, note that the logical layer depicted in Figure 1 (as layer 1) can tie together disparate physical networks and applications.



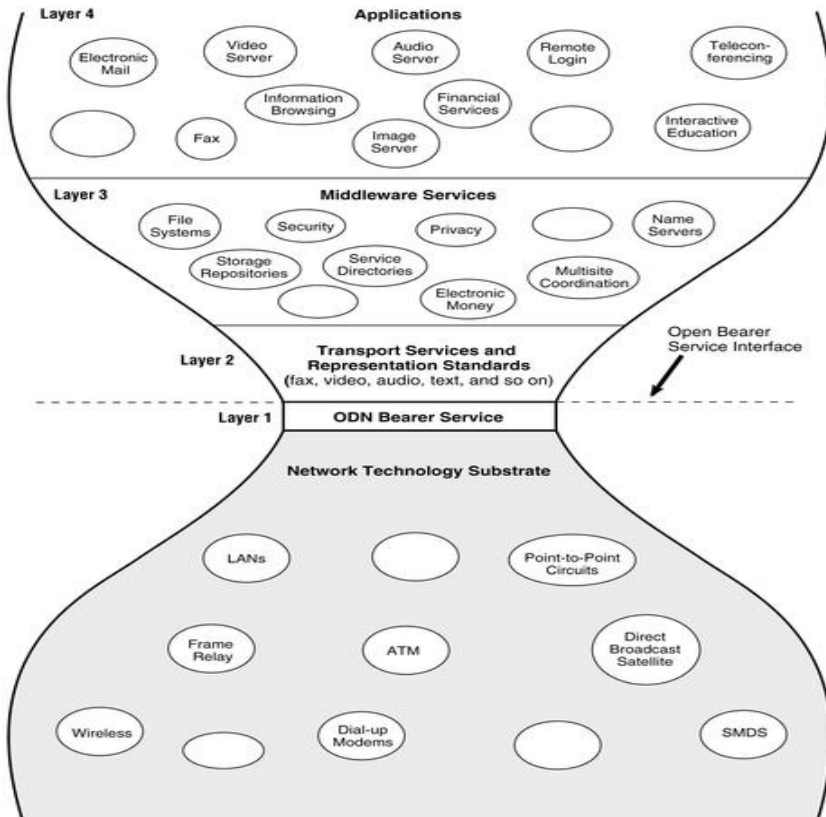


Figure 1: A Four Layer Model for an Open Data Network

Source: Computer Science and Telecommunications Board (CSTB), *Realizing the Information Future: The Internet and Beyond* (Washington, D.C.: National Research Council, 1994)

The basic Internet-enabled architecture major corporations use relies on a broadband access network that is connected to an Internet backbone network and is managed by “core application services.” Significantly, this architecture does not necessarily mean that the corporation relies on the public Internet at all. Instead, by using Internet technology (sometimes referred to as an “Intranet” system), corporations can manage their own private networks, connecting their branch offices, supply chain partners, and customers. Such a network, however, would not make available all applications to all users who connect to the network; customers would not be entitled to view payroll information, for example. Instead, it would use a system of “rights management” to limit who could query what information stored on a shared system. In the context of public safety, police officers would have access to a gang database, but ambulance services would not need such access. To outline the overall structure of such a system, Figure 2 describes the relationship between transport networks, data standards, core services, agency applications, and the overall policies and protocols that govern the use of the system.

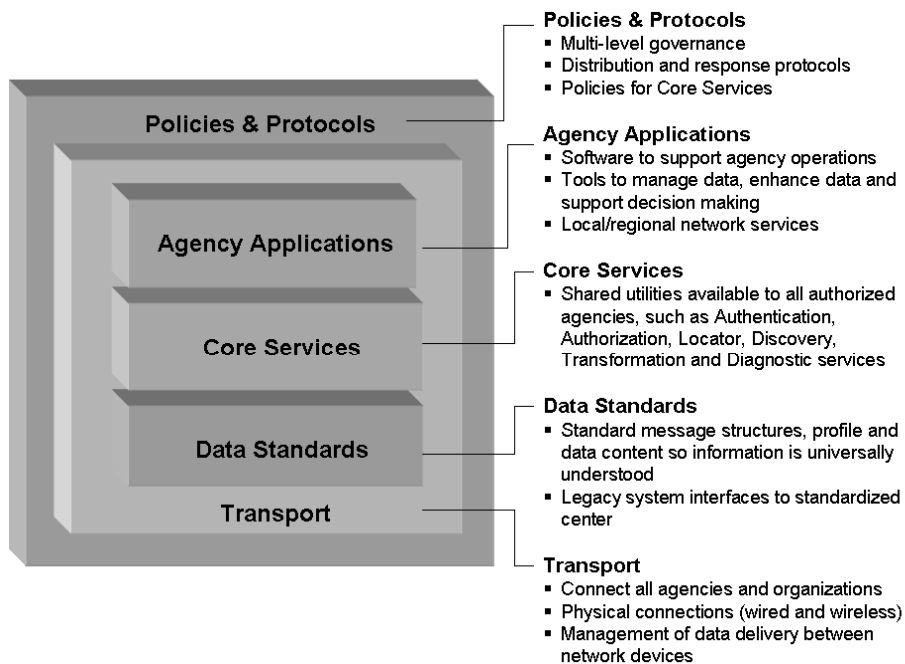
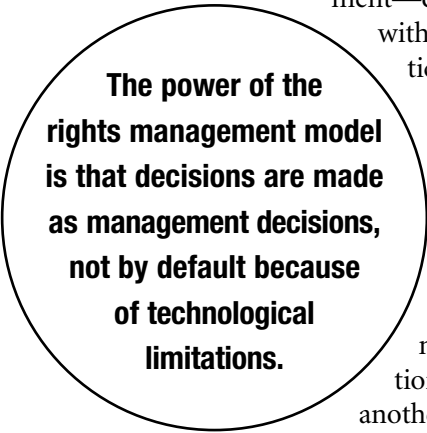


Figure 2: Model of a basic rights management system

To many nontechnologists, Figure 2 does not convey how a system based on Internet technology and open standards provides a platform for innovation and creativity. This platform, however, is fundamentally different from (and superior to) today's specialized systems, which provide little opportunity for customization, evolution, or innovation. Significantly, this model allows—within a shared network environment—different agencies to make decisions



**The power of the rights management model is that decisions are made as management decisions, not by default because of technological limitations.**

within their area of responsibility. In particular, a system of rights management can authenticate who is a permitted user and what access to information that user is entitled to—regardless of what underlying network they are using. Moreover, a basic rights management system can be customized so that in one jurisdiction the fire department might choose to share information with the local electric utility and, in another jurisdiction, it might choose not to share such information. The power of this model is that such decisions are made as management decisions, not by default (and hard-wired in) because of technological limitations. Consequently, as Kevin Kahn of Intel emphasized, such a network can easily accommodate and allow access for entities that may seem peripheral to emergency response and the safety enterprise (e.g., the power company), but can be crucial participants in resolving a particular emergency situation.

Figure 2 depicts an architecture that has yet to be fully developed. For example, the set of standards being used by commercial firms is unlikely to meet all of the needs of public safety agencies. Consequently, once the move to this architecture picks up speed, one would expect that the

public safety community would drive the development of new standards to facilitate applications that meet their particular needs.<sup>12</sup> As Kevin Kahn explained, new Internet standards “operate based on a proof of concept model that can meet a need” and use “an iterative approach as opposed to developing all of the possible requirements at once.” To begin, however, Kahn recommended “using existing systems and seeing what works.” Jennifer Warren, Senior Director of Trade and Regulatory Affairs for Lockheed Martin, built on this suggestion, noting that the military recognizes the value of a “systems integration approach” in which the focus often is on solutions, not specific technologies. This model allows for a system of “spiral development,” enabling ongoing integration of new, proven technologies into a system built on legacy systems. Significantly, the U.S. Department of Homeland Security (DHS) has been moving in this direction recently, including in developing a Statement of Requirements.<sup>13</sup>

The effort to adapt Internet technology to enable public safety agencies to communicate more effectively is just beginning and could take different directions. One near-term solution, advanced by Cisco, would connect existing radio systems into an IP gateway.<sup>14</sup> Longer-term solutions depend on build-out of broadband communication systems—either through a commercial provider that also serves other customers (to build greater economies of scale) via a dedicated high-speed wide area broadband technology (e.g., EV-DO) or through a wi-fi or WiMAX-based solution.<sup>15</sup> Significantly, however, an Internet-based architecture would be modular and flexible, so different agencies could all interoperate while experimenting with different broadband access solutions. Moreover, by using technologies such as multi-mode radios, public safety agencies can incorporate their legacy technologies into a broader architecture that would work alongside new broadband systems that could even include a satellite overlay component.<sup>16</sup>

### **III. Transforming Public Safety Communications**


The balkanized system of public safety communications reflects not technological limitations per se but the challenge of changing a culture whereby each local agency jealously safeguards its own purchasing prerogatives.<sup>17</sup> “The people part of the equation is 90 percent of the problem,” reported Charles Werner of the Charlottesville Fire Department. “It’s a control issue. Each agency has its own channels and is unwilling to give them up. This dates back to the building of each of these systems individually.” In essence, the prevailing cultural norm is that the police don’t want to take orders from firefighters, and vice versa—meaning that if either agency controls its own communications infrastructure, the other is not about to be subservient on matters of equipment purchasing or maintenance. Unfortunately, as Hank Hulquist, Assistant Vice President of Regulatory Planning & Policy for AT&T, added, the current system of spectrum allocation and assignment only reinforces this norm and the current model. By dividing spectrum into locality- and agency-specific licenses that are given away in a manner that discourages more efficient use (for example, by not providing a right to lease the spectrum to others), the current system of spectrum management creates the illusion that there is no cost to amassing spectrum or operating one’s own wireless network (and broader information and communications technology).

One systemic problem with public safety communications networks is that local officials often decide how to design and operate their own private networks without any incentive to coordinate with adjacent networks, which are similarly designed in isolation. In a more rational system, David Aylward of COMCARE emphasized, local fire chiefs, for example, would not operate private networks; they would use virtual private networks (VPNs) on a shared physical infrastructure. Some states, such as Virginia, have already begun to move in this direction,

developing a statewide wired IP-based network that can carry all emergency communications. In practice, such networks will be able to serve a variety of needs, with network management functions served by the relevant applications and controlled (through rights management) by local officials. Such a system would enable interoperability at the applications layer (as opposed to at the physical layer) and would rely on a system of rights management.

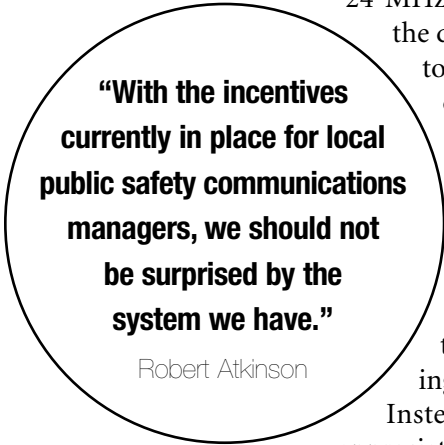
Fortunately, policymakers recognize the compelling nature of this vision, explained John Kneuer, Acting Assistant Secretary of Commerce for Communications and Information of the National Telecommunications and Information Administration (NTIA). In fact, the President's Spectrum Policy Initiative highlights the need for enhanced coordination and recently embraced, as a valuable demonstration project, the Wireless Accelerated Responder Network (WARN) project, which provides broadband access to a variety of agencies and permits interoperable, city-wide, real-time video tools for remote surveillance and detection.<sup>18</sup> Unfortunately, policymakers have yet to embrace an effective strategy to create incentives for local jurisdictions to cooperate more effectively on a systematic basis.

A critical challenge moving forward is charting a transition to a new model for public safety communications. The current focus, as Howard Woolley of Verizon Wireless reminded AIRS conferees, stems



**Policymakers will need to understand that the twin “fixes” of more spectrum and more money will not address the current failings of public safety communications.**

from the Deficit Reduction Act of 2005, which is the most recent “plan of record” on public safety interoperability from Congress and the administration. In essence, that model focuses on providing more money—\$1 billion for interoperability grants—and more spectrum—



**“With the incentives currently in place for local public safety communications managers, we should not be surprised by the system we have.”**

Robert Atkinson

24 MHz of spectrum cleared as a result of the digital television (DTV) transition—to address the failings of public safety communications. As the hard date for the DTV transition (February 17, 2009) approaches, however, others have argued that policy-makers will need to understand that the twin “fixes” of more spectrum and more money will not, by themselves, address the current failings of public safety communications. Instead, as Congress is beginning to appreciate,<sup>19</sup> a new vision for how technology will be used and more assertive federal and state leadership will be necessary to migrate toward a next-generation system for public safety communications.

#### *A. The Centrality of Incentives*

“With the incentives currently in place for local public safety communications managers, we should not be surprised by the system we have,” explained Robert Atkinson, President of the Information Technology and Innovation Foundation. After all, “we don’t charge for spectrum, and there are no incentives for cooperation”—meaning that the behavior of public safety agencies is in line with the generally slow-

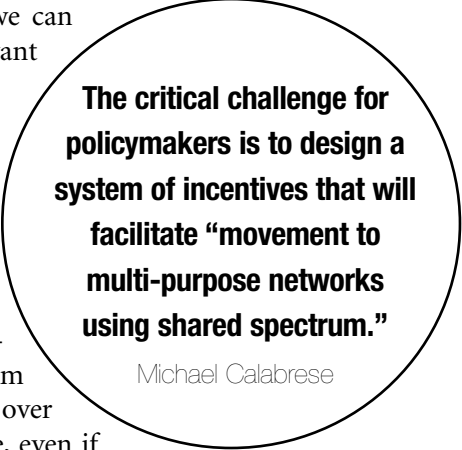


paced adoption of electronic communications by federal, state, and local governments and accounts for their relatively inefficient use of valuable spectrum. As Jennifer Warren of Lockheed Martin suggested, providing incentives for state-level engagement will prove most effective in promoting progress because the real challenges of fragmentation and management will not be solved by extracting fees from the public safety community. In any case, AIRS conferees agreed that once the incentives change, we can expect the behavior of the relevant managers to change.

In many respects, the state of public safety communications stems from a classic “principal-agent problem.” In particular, the central motivating force for the behavior of most local officials is to continue operating in an environment that is comfortable to them to maintain their perceived control over

the communications infrastructure, even if the result is an inferior technological system that compromises the effectiveness of public safety agencies. As Tom Hazlett of GMU noted, this dynamic is what makes the public safety communications problem so tragic. In particular, there are complementary interests and rights that could be combined for the good of the public, but the self-interests of individual managers are highly divergent, so forging cooperative arrangements is difficult.

The critical challenge for policymakers is to design a system of incentives that will facilitate “movement to multi-purpose networks using



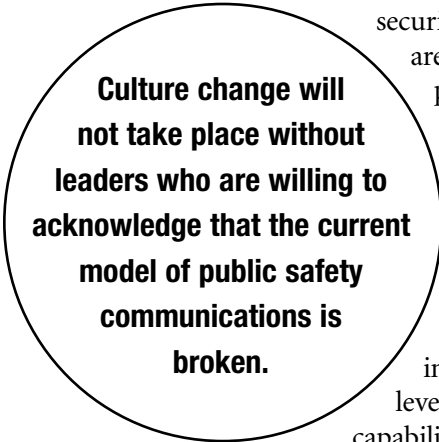
**The critical challenge for policymakers is to design a system of incentives that will facilitate “movement to multi-purpose networks using shared spectrum.”**

Michael Calabrese

shared spectrum,” concluded Michael Calabrese, Vice President and Director of the Wireless Future Program at the New America Foundation. Confronted with an option to move to multi-purpose, Internet technology-enabled networks, local public safety officials often

invoke concerns over network reliability and security. These concerns, however, often

are more myth than reality. For example, large numbers of critical mission networks rely on commercial off-the-shelf (COTS) equipment and commercial networks that use Internet technology. Moreover, the flexibility of such networks, particularly when they are part of an extensible architecture that includes legacy equipment, promises levels of redundancy that far exceed the capability of current networks.



**Culture change will not take place without leaders who are willing to acknowledge that the current model of public safety communications is broken.**

The AIRS conferees recognized that the incentives must overcome the culture of resistance. As Charles Werner of the Charlottesville Fire Department explained, the history of fiefdoms within the respective agencies obscures “gains from cooperation.” In many cases, managers of legacy radio systems tell chiefs that “you need to stick with the traditional land mobile radio system” or the system won’t remain secure. To be sure, education and demonstration projects are part of the answer because there is a basic lack of understanding about how modern networks are designed and managed—for example, security typically stems from effective encryption, not physically separate networks. Yet education alone will not do the trick. As Chief Werner recounted from his experience, getting beyond the silo-based approach is starting to

happen where incentives for cooperation—in the form of federal grants—create opportunities to bring together groups of distinct agencies and individuals through consensus-building leadership.

The ideal strategy marries economic incentives with courageous leadership. Culture change will not take place without leaders who are willing to acknowledge that the current model of public safety communications—particularly contrasted with the considerable opportunities for technological improvements—is broken. In some pockets of the country, leaders with appropriate economic incentives have risen to the challenge of addressing the balkanized public safety environment. Similarly, the world of E-911, which is riddled with a related set of problems based on local authorities operating their own call centers and using antiquated technology,<sup>20</sup> also has seen a few notable reform efforts that merit attention. Consider, for example, the case of Tim Barry, the Treasurer of Indiana. As Robert Pepper of Cisco reported, Barry convened a series of meetings with affected stakeholders to improve emergency communications. In so doing, Barry made clear his desire to see a more effective system put in place and, after developing the appropriate specifications, awarded a bid to a consortium that developed a unified IP platform—using voice over IP (VoIP) and modern IP technology—to manage a statewide E-911 network. Over time, such cases should become the norm, and islands of local authority making independent network decisions should become the exception.

### *B. Toward Effective Allocation of Responsibility*

“People are willing to invest money to support enhanced public safety communications,” Brian Fontes, Vice President of Federal Relations for Cingular Wireless, commented. Unfortunately, “the lack of a centralized management structure—especially with respect to technology specifica-

tion and acquisition—means that limited resources are spent in an uncoordinated and less efficient manner,” and we continue to make only minimal progress. Because federal grants have largely followed the model of allowing local agencies to dictate their purchasing priorities, the federal government has failed to prod states and localities toward a new, consistent

technological architecture. Consequently, as the House of Representatives Committee Investigating the Katrina Disaster concluded, “State and local governments [continue to be] responsible for designing and coordinating their efforts, and [have] failed to make meaningful progress *despite knowledge of the problem for years and the expenditure of millions in federal funds.*”<sup>21</sup>



**The goal of a next-generation architecture is to provide localities with greater tools and flexibility without having to manage the underlying technology.**

To spur the significant culture change required to adopt a new technological model, the federal government must adopt a more proactive stance on (1) embracing the type of architecture outlined in this report; (2) encouraging state leadership and coordination to spur that transition, including use of accountability metrics to ensure that federal funds are spent effectively; and (3) supporting demonstration projects, new standards development activity, and publicity for best practices. This type of role for the federal government best leverages its strengths—in particular, its control of funds and spectrum—and empowers state and local governments to adapt their responses to local circumstances.

After detailing the proposed action plan for the federal government, we discuss the proposed responsibilities for state and local govern-

ments. At the outset, we emphasize that this division of responsibility follows from four basic principles:

1. Emergency response is a local activity that must remain local. In particular, local public safety agencies must remain in control of information and communications systems at the logical/functional layer so they can perform their duties effectively. Therefore, the goal of a next-generation architecture is to provide localities with greater tools and flexibility to meet their particular needs—without having to manage the underlying technology.
2. States (or regional authorities) should manage or oversee the underlying network functions so that they are effective, are interoperable, and provide the necessary core services.
3. The federal government should provide significant resources—management, monetary support, spectrum, and support for development of standards by representative leaders and stakeholders—to promote a next-generation system of public safety communications and information management through incentives and accountability.
4. The federal government should work with all relevant stakeholders to develop a system of agreed-upon outcomes and metrics to measure progress.

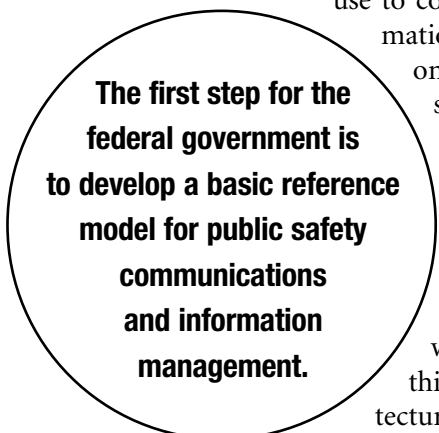
### *1. The Federal Government's Role*

The federal government must move beyond the model of simply providing spectrum and funds to local authorities. The current model,

left undisturbed, will result in more tragic results based on a cultural mindset that is rooted in a balkanized communications ecosystem. Thus, we recommend that the federal government commit to a series of steps that will result in adoption of a new technological model and the abandonment of the old mindset.

*a. Defining a Next-Generation Architecture*

The first step for the federal government is to develop a basic reference model (based on the network-of-networks concept) for public safety communications and information management. This model would outline the basic architecture that public safety agencies would use to communicate and manage their information needs. This system would not be a one-size-fits-all model; it would leave some discretion to state and local authorities. It would specify, for example, that a broadband access link is critical, but it would not dictate what type of technology or strategy (commercial vendor, municipally operated wireless network, etc.) should be used to provide this link. By specifying the basic architecture, premised on the network-of-networks model, the federal government could begin to move the public safety community in a direction that is more consistent with the current (valuable) effort by SAFECOM.<sup>22</sup>



**The first step for the federal government is to develop a basic reference model for public safety communications and information management.**

With a reference model in mind, the federal government should develop a hierarchy of critical steps for individual state-led systems to

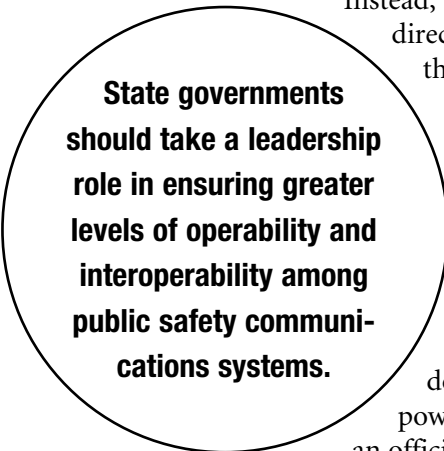
embrace. This hierarchy would take the form of a set of envisioned outcomes and specific metrics that would be used to measure progress. The federal government is well positioned to bring together affected stakeholders to identify available technologies and best practices that could inform such an action plan. Again, this action plan would not require abandonment of legacy systems or a one-size-fits-all solution, but it would require migration toward an overall flexible and extensible architecture that leverages technologies currently being used by commercial firms.

To do its part, the FCC should gear its spectrum policy decisions to spur adoption of the architecture outlined above. First, the Commission should ensure that any decision to award spectrum licenses to local agencies is conditioned on participation in a state or regional plan to migrate to a next-generation architecture. Second, the FCC should investigate possible strategies for facilitating development of a next-generation broadband, interoperable architecture. Such strategies could include, but need not be limited to, (1) implicit requirements imposed on spectrum licenses; (2) a broadband public trust model like that proposed by Cyren Call (which would require providing a broadband service to public safety in return for receiving spectrum licenses for free);<sup>23</sup> (3) incentives for public safety to use commercially available broadband networks; and/or (4) allowing public safety licensees to surrender spectrum in return for auction revenues that would be dedicated to technological upgrades and adoption of commercially available technology. Third, the Commission should investigate strategies for better organizing the planned assignment of additional safety spectrum in the upper 700 MHz band to enable broadband networking, either on spectrum dedicated to public safety alone or in a manner that would integrate with commercially available spectrum. Finally, the FCC should consider allowing secondary markets for public safety users, thereby allowing

users to both access and lease spectrum pursuant to secondary market rules. In particular, allowing public safety spectrum to be leased—for example, on an interruptible basis—could raise additional revenue, create robust networks with enhanced functionality, and reveal the opportunity costs of leaving this spectrum inefficiently used.<sup>24</sup>

*b. Encouraging State Leadership*

The federal government should no longer provide funds directly to local agencies. Such a strategy only invites and facilitates the lack of cooperation that has plagued public safety communications to date.



**State governments should take a leadership role in ensuring greater levels of operability and interoperability among public safety communications systems.**

Instead, the federal government should work directly with state governments to spur them to take a leadership role in ensuring greater levels of operability and interoperability among public safety communications systems.<sup>25</sup> Over time, money and spectrum provided to states should be conditioned on development of a coordinated strategy and the effective management required to make it happen. In so doing, the federal government can create powerful incentives for states to authorize an official—for example, a state chief information officer (CIO)—to facilitate cooperation and development of an integrated strategy.

The federal government should publicize its findings with regard to state progress and ensure that states are held accountable by the court of public opinion. Over time, after some states begin to lead the way in



migrating toward a new technological architecture, the federal government can act as a referee of yardstick competition between states and enable transparent assessments of how different states are progressing toward a next-generation architecture. For example, when 40 states have adopted IP backbone networks that connect all public safety agencies, E-911 calls, and others working in conjunction with first responders (e.g., ambulance dispatch services), there will be considerable pressure on the 10 remaining states that have yet to do so. Moreover, the federal government should perform regular audits to evaluate which states are using communications and information technology effectively.

### *c. Supporting Technological Development*

Finally, the federal government should build on and enhance the work spearheaded by SAFECOM, support demonstration projects, publicize best practices, and spur new standards development activity. One valuable vehicle for doing so is to ensure that the federal government's own disparate agencies are following a coordinated and integrated policy. To that end, the Office of Management and Budget (OMB) is well positioned to spur the various federal agencies to embrace the next-generation architecture outlined above.

The federal government also can and should play a critical role in assisting in developing standards and, ultimately, technologies that will support a next-generation architecture. To some degree, the FCC can help in this area by generally encouraging experimentation and development of technologies—even if they are being trialed by commercial firms—that can enable more effective public safety communications. These technologies include software-defined radio systems that might facilitate effective multi-mode radios, mesh networking systems (such as those being deployed using unlicensed spectrum), hybrid satellite-terres-

trial wireless systems, broadband data satellite services, and high-speed, wide area wireless technologies that generally are referred to as 3G and 4G systems. More broadly, the federal government should publicize developing technologies and the best practices for using them effectively.

Development of new standards to support public safety-centered applications is likely to be another area where the federal government's leadership will be particularly valuable. For example, the federal government can assist in the development of standards for core services and act as a repository for existing standards and other shared tools. For agencies with limited resources, the federal government should commit to support development of application service providers that host solutions—such as IP computer-aided dispatch (CAD) and mapping systems—that agencies can access over broadband Internet connections.

## *2. State Governments*

The critical role for state governments is to develop the skills needed to oversee an integrated emergency communications strategy. Ideally, this strategy would take a broad view of emergency response, including the current state of E-911 technology. In any event, it certainly would include developing shared resources where appropriate and ensure that all federal and state funds were invested to advance migration to a next-generation architecture.



**The critical role for state governments is to develop the skills needed to oversee an integrated emergency communications strategy.**

As the Indiana E-911 example makes clear, effective state leadership can make an enormous difference in driving adoption of advanced technolo-

gies that will provide for greater functionality and affordable systems. To spur such effective leadership, each state should appoint a single official (e.g., the state CIO or an emergency management head) to oversee development of a statewide plan to migrate toward a next-generation architecture. Based on the efforts of some states to better leverage the use of information and communications technology through an empowered and centralized CIO (where all IT employees work for a single agency), there are strong reasons to believe that such a model can succeed in this area.<sup>26</sup>

### *3. Local Governments and Public Safety Agencies*

Public safety agencies play a crucial role in responding to all forms of emergencies. Without effective communication systems, however, they often are doomed to respond ineffectively. To ensure effective emergency communications, public safety agencies should act more like enterprise customers, requiring certain functionalities and not specifying particular technologies that they must control and maintain. State or federal agencies can move to this model by developing requests for proposals and requirements documents that can be used by local agencies to procure the necessary services and take advantage of shared investments in information and communications technology. Increasingly, local public safety agencies are ill-prepared to judge the potential of modern technology—let alone to integrate it effectively. To be sure, the “last mile” connec-




**Public safety agencies should act more like enterprise customers, requiring certain functionalities and not specifying particular technologies.**

tions—that is, the broadband access links—must remain locally provisioned, but even in that area cooperation can enable local agencies to benefit from technological improvements. In short, by focusing their attention on their core needs and competencies, local agencies can ensure that their communications and information needs are met, even if they are not physically operating all of the relevant infrastructure to make it happen.

#### IV. Conclusion

The system whereby local agencies operate their own information and communications technology to support their emergency services is a relic of an antiquated technological model. This relic, unfortunately, is reinforced by prevailing cultural norms, current spectrum policy, the lack of incentives to migrate to a new model, and decentralized management. Over the past decade, major enterprises

and the military have adopted IP-based technology, developing a network-of-networks architecture that provides them with considerable flexibility and economies of scale. There is every reason to believe that public safety agencies can benefit from such a system. They simply need a reason and a roadmap to get there.



**“The future success  
of public safety lies in  
cooperation with the  
commercial world.”**

Chief Werner

The federal government is in a unique position to facilitate the transition to a next-generation architecture for public safety communications. At present, the federal government is not effectively using its ability to lead with conditioned funding and spectrum licenses, an articulated vision with milestones and metrics, and its ability to spur

and publicize technological solutions. By embracing this opportunity, the federal government can empower state governments to begin to oversee development of the systems needed to support effective public safety communications. To be sure, shifting to a new model for public safety communications needs will not be easy, but the objective of ensuring that our public safety personnel have the best available communications capabilities must be achieved.

The sooner all parties realize the opportunities available to public safety by adopting an IP-based architecture, the closer we will be to a system of interoperable, highly functional, and efficient public safety communications. There is reason for hope and optimism on this score. As Chief Werner of the Charlottesville Fire Department explained, “The future success of public safety lies in cooperation with the commercial world. Once people have seen it demonstrated, they will come.” He added, “Having purchased a multimillion-dollar radio system to operate privately—with all of the time-consuming, technically challenging, and financially burdensome process it entails—leaves me with the feeling of never wanting to do it again.” The challenge is creating the system of incentives and education to transform public safety communications. This transition will not happen overnight, but it is vital to our national well-being that it happen as soon as practicable.

## Endnotes

1. See [www.whitehouse.gov/reports/katrina-lessons-learned/chapter1.html](http://www.whitehouse.gov/reports/katrina-lessons-learned/chapter1.html).
2. Michael Chertoff, Remarks at the Tactical Interoperable Communications Conference (May 8, 2006), available at [www.dhs.gov/dhspublic/display?content=5596](http://www.dhs.gov/dhspublic/display?content=5596).
3. See William Pessemier, *Top Priority: A Fire Service Guide to Interoperable Communications*, 2 (International Association of Fire Chiefs, 2005), available at [www.interoperability.publicsafety.virginia.gov/Library/PDFs/FireService-InteropHandbook.pdf](http://www.interoperability.publicsafety.virginia.gov/Library/PDFs/FireService-InteropHandbook.pdf) (warning before Hurricane Katrina that despite “numerous after-action reports, public safety services have yet to make significant progress in comprehensively addressing interoperability”).
4. The Project 25 initiative, spearheaded by the Association of Public Safety Communications Officials (APCO) and supported by the Telecommunications Industry Association (TIA), has sought to craft a set of open standards that would invite entry and facilitate interoperability in the world of public safety communications. See *What Is Project 25?* available at [www.project25.org/display.php?file=content/WhatIs/p25.htm](http://www.project25.org/display.php?file=content/WhatIs/p25.htm).
5. Thomas W. Hazlett, “Katrina’s Radio Silence,” *Financial Times*, October 24, 2005.
6. Linda K. Moore, *Public Safety Communications: Policy, Proposals, Legislation and Progress*, CRS Report for Congress 17 (June 2005), available at [www.fas.org/sgp/crs/homesecc/RL32594.pdf](http://www.fas.org/sgp/crs/homesecc/RL32594.pdf) (stating that advanced communication technology is “typified by the near-ubiquity of the Internet and the wide availability of advanced wireless telephone” services, suggesting the possibility of “a world of end-to-end communications for public safety”); *FCC Report to Congress: On the Study to Assess Short-Term and Long-Term Needs for Allocations of Additional Portions of the Electromagnetic Spectrum for Federal, State and Local Emergency Response Providers*, 2005 WL 3618426 at ¶ 2 (F.C.C.) (December 19, 2005) (“there may now be a place for commercial providers to assist public safety in securing and protecting the homeland”); Jon M. Peha, “Protecting Public Safety With Better Communications Systems,” *IEEE Communications* (March 2005), available at [www.com-soc.org/ci1/Public/2005/Mar/cireg.html](http://www.com-soc.org/ci1/Public/2005/Mar/cireg.html) (stating that “the United States should reevaluate the traditional separation between public safety systems and commercial systems”).
7. National Reliability and Interoperability Council VII, Focus Group 1D, Communications Issues for Emergency Communications Beyond E-911, 3 (December 2005), available at [www.nric.org/meetings/docs/meeting\\_20051216/FG1D\\_Dec%2005\\_Final%20Report.pdf](http://www.nric.org/meetings/docs/meeting_20051216/FG1D_Dec%2005_Final%20Report.pdf).
8. John Peha, *How America’s Fragmented Approach to Public Safety Wastes Money and Spectrum* (September 2005), available at [http://web.si.umich.edu/tprc/papers/2005/438/Peha\\_Public\\_Safety\\_Communications\\_TPRC\\_2005.pdf](http://web.si.umich.edu/tprc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf).

9. Statement of Kevin J. Martin, Hearing on Communications in a Disaster, 7 (September 22, 2005), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-261219A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261219A1.pdf).
10. Presentation of Kenneth Moran, Director, Office of Homeland Security, Enforcement Bureau Agenda Meeting of the Federal Communications Commission (September 15, 2005), available at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-261112A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-261112A1.pdf).
11. This solution mirrors that called for by NRIC VII Focus Group 1D, which suggested that:

[a] single, interconnected Internet Protocol system should be used for all emergency communications, connecting a wide variety of agency-run and public networks, both wireline and wireless. Focus Group 1D calls this an “Inter-network” to emphasize that this group does not believe a new physical network is needed. It is a systems of systems approach.

National Reliability and Interoperability Council VII, Focus Group 1D, Communications Issues for Emergency Communications Beyond E-911 7 (December 2005), available at [www.nric.org/meetings/docs/meeting\\_20051216/FG1D\\_Dec%2005\\_Final%20Report.pdf](http://www.nric.org/meetings/docs/meeting_20051216/FG1D_Dec%2005_Final%20Report.pdf).
12. One such effort involves a coalition of first responders that is working to develop an eXtensible Markup Language (XML)-based standard (the Emergency Data Exchange Language (EDXL)) to enable the panoply of different agencies that might be called to the scene of an accident (e.g., public safety, transportation, and medical personnel) to share information with one another. See Diane Frank, “First Responders Seek Common Lingo,” *Federal Computer Week* (March 15, 2004), available at [www.fcw.com/article84556](http://www.fcw.com/article84556).
13. K.C. Jones, “Emergency Responders Can’t Communicate, DHS Warns,” *TechWeb* (May 11, 2006), available at [www.techweb.com/wire/security/187202152](http://www.techweb.com/wire/security/187202152) (noting that DHS “will set functional requirements and performance standards”); see also “Homeland Security First to Define Interoperability Requirements for Nation’s First Responder Community,” DHS press release (April 26, 2004), available at [www.dhs.gov/dhspublic/display?content=3513](http://www.dhs.gov/dhspublic/display?content=3513).
14. See *Solutions for Communications Interoperability*, Cisco Systems white paper, 2-3 (2005), available at [www.cisco.com/en/US/products/ps6718/products\\_white\\_paper0900aecd80350fee.shtml](http://www.cisco.com/en/US/products/ps6718/products_white_paper0900aecd80350fee.shtml).
15. There are a variety of models and visions for how such broadband access networks could be developed using emerging wireless technology. See Tropos Networks, “Metro Scale Video Surveillance: High-Profile Criminal Trial” (August 2004), available at [www.tropos.com/pdf/peterson\\_casestudy.pdf](http://www.tropos.com/pdf/peterson_casestudy.pdf) (discussing Tropos’ mesh networking wifi solution); Robert Hoskins, “Alvarion to Deliver Wireless and WiMax for Public Safety,” *Broadband Wireless Exchange* (May 11, 2006), available at [www.bbwxchange.com/publications/page1423-137445.asp](http://www.bbwxchange.com/publications/page1423-137445.asp) (discussing Alvarion’s solution using WiMAX).

16. For a discussion of how such a system could work, see Philip J. Weiser et al., “Toward A Next Generation Architecture for Public Safety Communications,” available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=903151](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903151).
17. As Jon Peha notes, the United States has never developed a coherent architecture for public safety communications infrastructure, nor even a meaningful national strategy that would lead to close coordination of the more than 50,000 U.S. public safety agencies and a commonly accepted set of objectives. Obviously, without effective coordination mechanisms, any communications infrastructure designed by many thousands of independent decisionmakers is prone to producing a tangle of systems that do not interoperate.  
  
John Peha, “How America’s Fragmented Approach to Public Safety Wastes Money and Spectrum,” 2, paper presented at 33rd Telecommunications Policy Research Conference (September 2005), available at [http://web.si.umich.edu/tprc/papers/2005/438/Peha\\_Public\\_Safety\\_Communications\\_TPRC\\_2005.pdf](http://web.si.umich.edu/tprc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf).
18. Testimony of John M.R. Kneuer, Acting Assistant Secretary for Communications and Information, before the Committee on Homeland Security’s Subcommittee on Emergency Preparedness, U.S. House of Representatives (April 25, 2006), available at [www.ntia.doc.gov/ntiahome/congress/2006/Kneuer\\_interoperable\\_042506.htm](http://www.ntia.doc.gov/ntiahome/congress/2006/Kneuer_interoperable_042506.htm).
19. H.R. 5351, the National Emergency Management Reform and Enhancement Act of 2006, for example, would require that DHS develop the necessary voluntary consensus standards in three years to facilitate migration to a next-generation architecture. Moreover, the bill also calls for enhanced state leadership, in the form of interoperability plans.
20. See Dale Hatfield, “A Report on Technical and Operational Issues Impacting the Provision of Enhanced 911” (2002), available at [http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native\\_or\\_pdf=pdf&id\\_document=6513296239](http://gullfoss2.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6513296239).
21. See United States House of Representatives, *A Failure of Initiative: The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, 174 (February 15, 2006), available at [www.c-span.org/pdf/katrinareport.pdf](http://www.c-span.org/pdf/katrinareport.pdf) (emphasis added).
22. See *supra* note 18. In a model along the lines we envision, the NTIA has begun to develop “a long-term standardized approach for nationwide communications interoperability and information sharing among local, State, and Federal public safety agencies, and short-term interim solutions to facilitate communications while the long-term approach is being completed.” Testimony of John M.R. Kneuer, *supra* note 18.



23. The specifics of the Cyren Call proposal are set out at [www.cyrencall.com/downloads/CyrenCall\\_PetitionRulemaking.pdf](http://www.cyrencall.com/downloads/CyrenCall_PetitionRulemaking.pdf).
24. Joshua Marsh, "Secondary Markets in Public Safety Spectrum" (2004), available at <http://web.si.umich.edu/tprc/papers/2004/384/tprc.pdf>.
25. To be sure, some state governments already are moving in this direction (with support from the National Governors Association Policy Academy on Wireless Interoperability), but federal encouragement is critical to ensuring more consistent and effective leadership. See National Association of State Chief Information Officers, *We Need to Talk: Governance Models to Advance Communications Interoperability*, 2-3 (November 2005).
26. See, e.g., Tod Newcombe, "Leaving His Mark," Public CIO (November 2005), available at [www.public-cio.com/story.php?id=2005.11.08.97208](http://www.public-cio.com/story.php?id=2005.11.08.97208).



# **APPENDIX**





# P articipants

**Clearing the Air:  
*Convergence and the Safety Enterprise***

Aspen Wye River House  
Queenstown, Maryland  
May 3-5, 2006

**Robert D. Atkinson**

President  
The Information Technology  
and Innovation Foundation

**David K. Aylward, Esq.**

Director  
COMCARE  
and  
President  
National Strategies, Inc.

**Dean R. Brenner**

Vice President, Government Affairs  
QUALCOMM, Inc.

**Michael Calabrese**

Vice President and Director  
Wireless Future Program  
New America Foundation

**Fred Campbell**

Legal Advisor, Wireless Issues  
Federal Communications  
Commission

**David Don**

Senior Director,  
Spectrum Policy  
Comcast Corporation

**Charles M. Firestone**

Executive Director  
Communications and  
Society Program  
The Aspen Institute

**Brian Fontes**

Vice President  
Federal Relations  
Cingular Wireless

**Michael Gottdenker**

Chairman  
and  
Chief Executive Officer  
Access Spectrum, LLC

**Dale N. Hatfield**

Independent Consultant  
and  
Adjunct Professor,  
Interdisciplinary  
Telecommunications Program  
University of Colorado at Boulder

**Thomas Hazlett**

Professor of Law and Economics  
George Mason University  
School of Law

**Hank Hultquist**

Assistant Vice President  
Regulatory Planning and Policy  
AT&T

**Kevin Kahn**

Intel Senior Fellow  
and  
Director  
Communications Technology Lab  
Intel Corporation

**John M. R. Kneuer**

Acting Assistant Secretary of  
Commerce for Communications  
and Information  
National Telecommunications  
and Information Administration  
U.S. Department of Commerce

**Stagg Newman**

President  
Pisgah Comm Consulting

**Morgan O'Brien**

Chairman  
and  
Chief Executive Officer  
Cyren Call Communications

**Preston Padden**

Executive Vice President  
Government Relations  
The Walt Disney Company

**Robert Pepper**

Senior Managing Director  
Global Advanced  
Technology Policy  
Cisco Systems

**Steve B. Sharkey**

Director, Spectrum and Standards  
Strategy  
Motorola, Inc.

**Jennifer Warren**

Senior Director  
Trade and Regulatory Affairs  
Lockheed Martin

**Philip J. Weiser**

Professor of Law and  
Telecommunications  
and  
Executive Director, Silicon  
Flatirons Telecommunications  
Program  
University of Colorado

**Kevin Werbach**

Assistant Professor of Legal  
Studies and Business Ethics  
The Wharton School, University  
of Pennsylvania

**Charles Werner**

Chief  
Charlottesville Fire Department

**Howard Woolley**

Senior Vice President  
Policy and  
Government Affairs  
Verizon Wireless

*Staff:*

**Mridulika Menon**

Project Manager  
Communications and  
Society Program  
The Aspen Institute





# About the Author

**P**hil Weiser is a professor of law and telecommunications and founder and executive director of the Silicon Flatirons Telecommunications Program at the University of Colorado. Professor Weiser writes and teaches in the areas of telecommunications and information policy. He recently co-authored *Digital Crossroads: American Telecommunications Policy in the Internet Age* (MIT Press, 2005). Prior to joining the CU faculty, Professor Weiser served as senior counsel to the Assistant Attorney General in charge of the Antitrust Division at the United States Department of Justice, advising primarily on telecommunications matters. Before his appointment at the Justice Department, Professor Weiser served as a law clerk to Justices Byron R. White and Ruth Bader Ginsburg at the United States Supreme Court and to Judge David Ebel at the Tenth Circuit Court of Appeals. Professor Weiser graduated with high honors from the New York University School of Law in 1994 and Swarthmore College in 1990.



# Selected Publications

*from the Aspen Institute  
Communications and Society Program*

*First Informers in the Disaster Zone: The Lessons of Katrina*

Hurricane Katrina taught some hard lessons that a year later still reverberate through government, media and society. In the wake of America's worst modern disaster, a steady flow of news stories, articles, books, government reports, and public forums have built a literature that provides guidance to vital institutions in coping with future calamities. The goal of this report is to add to that knowledge by exploring how the disaster transformed the gathering and dissemination of crisis information. This topic was confronted by participants in a conference hosted by the Aspen Institute Communications and Society Program on May 17-19, 2006, in Queenstown, Maryland. Authored by Albert L. May.

Forthcoming 2006, \$15.00

*Policy Issues for Telecommunications Reform*

In these two reports, the author considers the changes that are necessary and appropriate to the Communications Act in view of technological convergence in the digital and network sectors, the changing economic and business circumstances of telecommunications users and providers, and the preservation of ongoing social policy. The reports also touch on how spectrum policies can address problems in rural telecommunications and broadcast services, and offer policy options for consideration in both the legislative and regulatory arenas. Authored by Robert M. Entman.

2005, 67 pages, ISBN Paper: 0-89843-445-9, \$15.00

*Reforming Telecommunications Regulation*

The report of the 19th Annual Aspen Institute Conference on Telecommunications Policy describes how the telecommunications regulatory regime in the United States will need to change as a result of technological advances and competition among broadband digital subscriber line (DSL), cable modems, and other players such as wireless broadband providers. Proposing major revisions of the Communications Act and FCC regulations, the report suggests an interim transitional scheme toward ultimate deregulation of basic telecommunications, revising the current method for universal service subsidies, and changing the way regulators look at rural communications. Authored by Robert M. Entman.

2005, 47 pages, ISBN Paper: 0-89843-428-9, \$15.00

*Challenging the Theology of Spectrum: Policy Reformation Ahead*

This report examines the theology of spectrum—that is, the assumptions and mythology surrounding its management and use. The report looks at how new technologies affecting spectrum, such as software-defined radio, can challenge the conventional wisdom of how spectrum should be managed. That innovation allows for access to unused frequency space or time on frequencies that are otherwise licensed to an exclusive user. Authored by Robert M. Entman.

2004, 43 pages, ISBN Paper: 0-89843-420-3, \$15.00

*Spectrum and Network Policy for Next Generation Telecommunications*

The report of the 18th Annual Aspen Institute Conference on Telecommunications Policy offers policy alternatives in both spectrum and network policy to achieve new gains for the telecommunications field. The

first essay suggests new management approaches to encourage more efficient uses of the spectrum while preserving the commitment to reliability of service and public safety values. The second essay debates the competitive structure of the telecommunications industry and its implications for building Next Generation Networks (NGN) and identifies three areas to encourage optimal development of the NGN: (1) operate the NGN on a price deregulated basis and begin addressing access regulation issues, (2) secure intellectual property rights of content suppliers, and (3) adjust the system of subsidized pricing to bring about competitively neutral pricing.

2004, 53 pages, ISBN Paper: 0-89843-394-0, \$12.00

*Balancing Policy Options in a Turbulent Telecommunications Market*

How does the country strike a balance between telecommunications deregulation and regulation in order to encourage appropriate levels of investment and competition? Should the U.S. adopt a more flexible, varied approach to spectrum policy that includes a mix of market solutions and government regulation? Are there new models of spectrum allocation and management that the government should consider? This report assesses the future of communications regulatory paradigms in light of desirable changes in spectrum policy, telecommunications market environments, and regulatory goals. It suggests four models of regulation, including government allocation, private spectrum rights, unlicensed commons, and a hybrid system of dynamic spectrum access. It also addresses how changes in spectrum and other telecommunications policies, and new business realities, might affect current regulatory regimes for the telecommunications industries. The publication includes an excellent background paper on spectrum policy by Dale Hatfield.

2003, 69 pages, ISBN Paper: 0-89843-370-3, \$12.00

*Telecommunications Competition in a Consolidating Marketplace*

In the telecommunications world, what would a fully competitive environment look like? What communications initiatives should policymakers develop—considering the ultimate welfare of the consumer—to implement change in the regulatory climate? This report explores ways to reshape the current regulatory environment into a new competitive space. It addresses competition not only within but across separate platforms of communications such as cable, wireline telephony, wireless, satellite, and broadcast. This publication also includes an essay on an innovative approach to wireless regulation, "Opening the Walled Airwave," by Eli M. Noam.

2002, 64 pages, ISBN Paper: 0-89843-330-4, \$12.00

*Transition to an IP Environment*

This report examines a "layered approach" to regulation. By viewing telecommunications in four separate layers—content, application, network, and data link—policy discussions can address concerns in one layer without negatively affecting useful existing policy in other layers. Also presented are beliefs that the growth of broadband should prompt a new discussion about universal service reform. The report also includes "Thoughts on the Implications of Technological Change for Telecommunications Policy," by Michael L. Katz. Authored by Robert M. Entman.

2001, 78 pages, ISBN Paper: 0-89843-309-6, \$12.00

*Six Degrees of Competition: Correlating Regulation with the Telecommunications Marketplace*

This report addresses the basic conceptual questions of what the nature of regulation should be in a competitive, broadband future. It also examines how fundamental policy issues such as interconnection, mergers, spectrum allocation, jurisdiction, universal service, and consumer protection

should be handled in the interim. The report also includes “Regulation: The Next 1000 Years,” by Michael L. Katz. Authored by Robert M. Entman. 2000, 65 pages, ISBN Paper: 0-89843-279-0, \$12.00

*Residential Access to Bandwidth: Exploring New Paradigms*

This report explores policy initiatives that would encourage widespread deployment of residential broadband services throughout the United States. It identifies our regulatory system as one of the chief obstacles to achieving ubiquitous broadband deployment and offers a new regulatory model to overcome these barriers. Authored by Robert M. Entman. 1999, 35 pages, ISBN Paper: 0-89843-256-1, \$12.00

*Competition, Innovation, and Investment in Telecommunications*

This report considers how public policy can foster investment, competition, and innovative services in local exchange telecommunications. The volume also includes “An Essay on Competition, Innovation, and Investment in Telecommunications,” by Dale N. Hatfield and David E. Gardner. Authored by Robert M. Entman.

1998, 52 pages ISBN Paper: 0-89843-235-9, \$12.00

*Implementing Universal Service after the 1996 Telecommunications Act*

This report summarizes the conference's suggestions for universal service policy options, generally, and financing options for schools and libraries, specifically, which were submitted to the Federal-State Joint Board on Universal Service in September 1996. The report includes an appendix with sections of the Telecommunications Act of 1996 that relate to universal service. \$10.00





# The Aspen Institute Communications and Society Program

[www.aspeninstitute.org/c&s](http://www.aspeninstitute.org/c&s)

The Communications and Society Program is a global forum for leveraging the power of leaders and experts from business, government, and the nonprofit sector in the communications and information fields for the benefit of society. Its roundtable forums and other projects aim to improve democratic societies and diverse organizations through innovative, multidisciplinary, values-based policymaking. They promote constructive inquiry and dialogue and the development and dissemination of new models and options for informed and wise policy decisions.

In particular, the Program provides an active venue for global leaders and experts from a variety of disciplines and backgrounds to exchange and gain new knowledge and insights on the societal impact of advances in digital technology and network communications. The Program also creates a multidisciplinary space in the communications policymaking world where veteran and emerging decision makers can explore new concepts, find personal growth and insight, and develop new networks for the betterment of the policymaking process and society.

The Program's projects fall into one or more of three categories: communications and media policy, communications technology and the democratic process, and information technology and social change. Ongoing activities of the Communications and Society Program include annual roundtables on journalism and society, international journalism, telecommunications policy, Internet policy, information technology, and diversity and the media. The Program also convenes the Aspen Institute Forum on Communications and Society, in which chief executive-level leaders in the business, government, and the nonprofit sector examine issues relating to the changing media and technology environment.

Conference reports and other materials are distributed to key policymakers and opinion leaders within the United States and around the world. They also are available to the public at large through the World Wide Web.