

Collaborative Networks and the Alaska Land Mobile Radio System: A Framework for Analyzing Inter-Agency People Problems Which Frustrate Public Safety Interoperability

J. Brad Bernthal, Steve Robertson and Justin Turner¹

ABSTRACT

Human factors are often emphasized as foremost among barriers to achieving interoperable communications. This paper places analysis of public safety interoperability in the broader discussion of collaborative networks, where entities bridge organizational boundaries, combine resources, and pursue joint goals. The paper focuses on tensions surrounding initiatives where an agency – typically an agency built to resolve problems within its jurisdictional boundaries – attempts to capture 21st Century network effects by working across jurisdictional boundaries. Issues arising from this tension – so-called “people-problems” – can be best understood through the prism of a coherent framework which identifies the risks and incentive-related problems of collaborative networks. We provide such a framework for public safety by identifying salient concepts such as risk factors, dimensions of trust, as well as principal-agent and collective action issues. Analyzed through this framework, the Alaska Land Mobile Radio System (“ALMR”) presents a notable case study: ALMR features inter-jurisdictional cooperation which has produced spectrum pooling, infrastructure sharing and interoperability across multiple agencies. While a laudable effort, however, our analysis indicates that it is dubious whether the ALMR model could be simply implemented wholesale in most parts of the United States. Nonetheless, ALMR’s 12-year history of interoperability efforts presents a rich study of “people problems” that is instructive for policy-makers seeking tools to achieve public safety interoperability.

INTRODUCTION

A ubiquitous theme in public safety discussions is that a broad range of people problems – not technology barriers – prevent interoperability. The perspective articulated by Homeland Security Secretary Michael Chertoff in 2006 is representative of a view shared by many policy-makers, public safety officials, and commentators:

“[T]he biggest barrier to interoperability is not technology . . . It has to do with, rather, human beings. It has to do with how do we get people to be able to use this equipment in a way that makes interoperability not just a theoretical possibility, or a technological possibility, but an actual, workable, day-to-day solution.”²

Notably, such people problems have proved nettlesome. In 2001, the United States

¹ Brad Bernthal (email: Brad.Bernthal@Colorado.Edu), Associate Clinical Professor, Colorado Law School, Adjunct Professor, Interdisciplinary Telecommunications Program, University of Colorado-Boulder; Steve Robertson, Major, United States Army, Master’s Candidate, Interdisciplinary Telecommunications Program, University of Colorado-Boulder; Justin Turner, Senior Network Systems Engineer, The MITRE Corporation. *The ideas and expressed herein are solely the authors’ and in no way reflect the official positions or opinions of the authors’ respective employers.* The authors would like to thank Nick Alexander, Dale Hatfield, and Phil Weiser for encouragement and thoughtful feedback and suggestions.

² Michael Chertoff, Homeland Security Secretary, Remarks at Tactical Interoperable Communications Conference (May 2006) (available at http://www.dhs.gov/xnews/speeches/speech_0281.shtm); see also U.S. Department of Justice and U.S. Department of Homeland Security SAFECOM Program, *2006 National Interoperability Summit Proceedings*, at 21, Prepared by SEARCH The National Consortium for Justice Information and Statistics (May 24-25, 2006) (available at <http://www.search.org/files/pdf/2006InteropSummitProceedings.pdf>) (resolving people problems across balkanized entities is difficult; “interagency and intra-agency dynamics can get in the way of the big picture of interoperable communications.”).

established SAFECOM with the goal of achieving nationwide interoperability among all first responders – federal, state and local – within 18-24 months. Six years later, notions of a quick switch to interoperability have given way to a more nuanced understanding that achieving public safety interoperability objectives requires surmounting formidable difficulties. To date, most public safety discussions have not recognized that similar issues attend many collaborative networking efforts involving government agencies. That is, most interoperability research and analysis to date examines interoperability as a *public safety-specific* problem rather than conceptualizing interoperability as part of the larger question concerning the challenges involved in creating effective *collaborative networks*. Notably, even outside of public safety contexts, “agencies are increasingly engaging in cross-boundary efforts, including horizontal partnerships between state agency-state agency, state agency-locality/tribal entity, state agency-federal government and public-private partnerships.”³ In this respect, first responder interoperability challenges are not *sui generis*: they share challenges with other networking efforts such as geographic information sharing of data across agencies,⁴ establishment of a cross-jurisdictional information sharing of justice information between law enforcement, prosecutors, public defenders, and courts,⁵ and collaborative networks assembled to respond to global health pandemics.⁶ Each of these types of collaborative network solutions is routinely stymied by human factors, including risk arising from inter-jurisdictional collaboration, lack of trust, principal-agent problems, and myriad disincentives to cross-agency cooperation.

Like most government entities, from their origins public safety agencies were not architected in a manner which anticipated 21st Century network capabilities. Notably, collaborative governance studies investigate the tensions engendered where agencies not architected for cross-agency cooperation seek to deploy collaborative networks. Significantly, the confluence of technological enablers such as increased processing power, enhanced memory, and longer-lasting power supplies have resulted in greater intelligence and capabilities “at the edge” of networks. This trend has helped “collaps[e] time and space”⁷ and ushered in an era where network capabilities far exceed those previously available.⁸ In short, a user at one end of a network can process unprecedented amounts of information while, concomitantly, connecting with other end users that can collect, share and provide unprecedented amounts of information. While governments cannot ignore the opportunity to leverage advanced networking capabilities, the purpose and structure of government entities presents unique challenges that resist some of the “flattening” effects more often seen in the private sector. Donald Kettl has observed that “[a]lthough public institutions are organized in hierarchies, they increasingly face difficult, non-routine problems that demand networked solutions.”⁹

³ NASCIO, *Getting Started in Cross-Boundary Collaboration: What State CIOs Need to Know*, at 1 (2007) (herein, “*What State CIOs Need to Know*,” available at <http://www.nascio.org/publications/documents/NASCIO-CrossBoundaryCollaboration.pdf>). For helpful study of trends concerning collaborative networks in government, see, e.g., Center for Technology in Government, University at Albany, SUNY, *New Models of Collaboration: An Overview* (October 2004) (available at http://www.ctg.albany.edu/publications/reports/new_models_exec).

⁴ Ophelia Englene and Sharon Dawes, *New Models of Collaboration: New York State GIS Coordination Program* (2003) (part of *New Models of Collaboration* study spearheaded by Center for Technology in Government at University at Albany, SUNY, materials available at http://www.ctg.albany.edu/publications/reports/new_models/new_models.pdf).

⁵ See *What State CIOs Need to Know* at 1 (discussing U.S. Department of Justice’s Global Justice Information Sharing Initiative – further information available at http://www.it.ojp.gov/topic.jsp?topic_id=8).

⁶ G. Edward DeSeve, *Business of Government Magazine*, *Creating Managed Networks as a Response to Societal Challenges*, at 48 (Spring 2007) (herein, “DeSeve,” available at <http://www.businessofgovernment.org/pdfs/forum07.pdf>).

⁷ John Kamensky, *Business of Government Magazine*, *Forum: Collaborative Governance*, at 45 (IBM Center for the Business of Government, Spring 2007) (available at <http://www.businessofgovernment.org/pdfs/forum07.pdf>);

⁸ See generally The Harvard Policy Group on Network-Enabled Services and Government, *Eight Imperatives for Leaders in a Networked World: Guidelines for the 2000 Election and Beyond* (John F. Kennedy School of Government) (available at <http://www-01.ibm.com/industries/government/ieg/pdf/eightImperative.pdf>).

⁹ *Business of Government Magazine*, *Forum: Collaborative Governance*, at 45 (IBM Center for the Business of Government,

This paper argues that it is useful to situate public safety interoperability issues within the larger discussion of how to better achieve effective cooperative governance through cross-boundary cooperation. This broader perspective allows public safety to draw upon additional relevant analyses, case studies, and recommended best practices which aim to resolve cross-jurisdictional collaboration issues similar to those which plague interoperability. In this paper, *cross-boundary collaboration* “is a process in which two or more entities agree to cross organizational boundaries and combine resources in order to achieve joint goals.”¹⁰ Specifically, the aim of such efforts is to successfully create *collaborative networks*, by which this paper means networks involving two or more entities where the public benefits of interconnecting the entities exceeds the costs of such interconnection. As a general matter, it should be noted that academic investigation concerning cross-boundary collaboration and study of collaborative networks is hardly complete and merits further work. As one commentator has noted, “we are only at the beginning of our understanding about how to create and invoke networks to accomplish public missions.”¹¹

By linking analysis of human factors involved in public safety interoperability with broader conversations concerning agency efforts to establish collaborative networks, this paper aims to make two contributions. First, we provide a framework which focuses on the risks and incentive-related problems implicated by collaborative networks. Development of a coherent analytic framework is useful in helping collaborative network participants anticipate and troubleshoot problems which, if undetected, could undermine an initiative. Second, as a case study, we provide a description of the Alaska Land Mobile Radio (“ALMR” or the “Project”) system and then situate ALMR within the larger context of collaborative network people problems. ALMR is highly relevant insofar as it partners federal, state and local governments in a cross-jurisdictional arrangement that features shared frequencies using trunking technology.¹² ALMR’s operational achievements are notable, however, they do not alone tell the complete story. ALMR’s 12-year history is replete with “people problems” endemic to collaborative network efforts. Some people problems have been adroitly addressed; others have been inadequately resolved. Indeed, even today, ALMR remains very much at an inflection point: there remains uncertainty as to whether ALMR will establish a viable way to fund the system and, moreover, whether large numbers of local users will join the completed system.

This paper proceeds in four parts. Following this Introduction, Part I provides an overview of the pernicious consequences of a lack of interoperability, such as operational limitations, spectrum scarcity, and over-built communications systems that are not cost-effective. Part II then draws upon existing research concerning collaborative networks to examine problems inherent in cross-jurisdictional collaboration. In particular, four factors – ranging from a lack of trust to collective action problems – are identified as explaining why people problems present formidable resistance to interoperability objectives. Part III provides a description of the Alaska Land Mobile Radio (“ALMR”) system and then analyzes ALMR within the framework of collaborative network efforts. Finally, Part IV concludes that, while a transition to next generation networks will be critical for public safety, such transition will not eliminate the importance of people problems going forward.

Spring 2007) (available at <http://www.businessofgovernment.org/pdfs/forum07.pdf>).

¹⁰ *What State CIOs Need to Know* at 1 (emphasis added).

¹¹ DeSeve, *supra* Note 6, at 52.

¹² *In the Matter of Applications of STATE OF ALASKA Request for Waiver of Sections 2.102(c), 2.103(a), 90.20, and 90.173(c) of the Commission’s Rules*, ¶ 1 (DA 03-2612, herein, “FCC Waiver Order”) (August 7, 2003). A trunked radio system operates on the same shared resources principle that the telephone network has used for many years. Frequencies in the system are pooled among users and then dynamically assigned on an “as needed” basis when there traffic to send for a particular user or group of users.

PART I. STATE OF PUBLIC SAFETY COMMUNICATIONS AND THE CONSEQUENCES OF INTER-JURISDICTIONAL COMMUNICATION COORDINATION PROBLEMS

Public safety communications challenges primarily emanate from the distributed nature of public safety agencies in the United States. Responders are distributed vertically (*viz.*, federal, state and local governmental levels), as well as horizontally (*viz.*, each layer of government features diverse disciplines of responders—e.g., police and fire at the local levels).¹³ Traditionally, first responder agencies developed their own communications networks. This has spawned a balkanized patchwork of systems that – while individually tailored to agencies’ specific needs – often do not operate well in combination with one another. Problems engendered by this lack of interoperability can be sorted into three broad categories: (i) operational limitations, (ii) spectrum scarcity and unsatisfactory network capabilities, and (iii) expensive communication systems that are not cost-effective.

A. What Is Interoperability?

A widely-accepted uniform definition of interoperability for public safety agencies does not yet exist.¹⁴ As reflected in Appendix A, however, a family of interoperability characteristics has emerged which – absent good reason warranted by the context – attends and defines the capabilities of robust interoperable public safety communications.¹⁵ These characteristics include (i) the ability of emergency response providers (and, often, other public service providers) to communicate between vertical governmental levels (*viz.*, federal-state-local);¹⁶ (ii) the ability of emergency response providers (and, often, other public service providers) to horizontally communicate across diverse disciplines of response resources (*viz.*, local-local agency communication);¹⁷ (iii) the ability to perform under a common command-and-control structure to achieve predictable results;¹⁸ (iv) access to networks that enable robust and real-time communications between responders, including voice, data, and video capabilities;¹⁹ and (v) the capability to rapidly authorize users without compromising secure communications.²⁰ While not often expressed in formal definitions of interoperability, discussions almost uniformly include a

¹³ Kiki Caruson and Susan A. MacManus *Designing Homeland Security Policy within a Regional Structure: A Needs Assessment of Local Security Concerns*, Journal of Homeland Security and Emergency Management, at 1 (Vol. 4 : Iss. 2, Article 7 (2007)) (available at: <http://www.bepress.com/jhsem/vol4/iss2/7>)

¹⁴ See, e.g., NASCIO Research Brief, *We Need to Talk: Governance Models to Advance Communications Interoperability* (November 2005) (herein, “*We Need to Talk*”) (“Interoperability has different meanings depending on the context”); see also the acknowledgment that expert participants in a recent Aspen Institute dialogue “spent some time arguing about the definition of ‘interoperability.’” *Aspen 2006 Emergency Communications*, Note 26 *supra*, at 3.

¹⁵ By “public safety,” this paper generally contemplates the breadth of agencies identified in a Congressional Research Service report. “Public safety agencies include the nation’s first responders (such as firefighters, police officers, and ambulance services) and a number of local, state, federal [including Department of Defense] — and sometimes regional — authorities.” Linda K. Moore, *Public Safety Communications: Policy, Proposals, Legislation and Progress*, at 1 (CRS Report for Congress, Updated June 8, 2005) (herein, “*June 8, 2005 CRS Report*,” available at <http://www.fas.org/sgp/crs/homesecc/RL32594.pdf>).

¹⁶ PL 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004. To prevent confusion, it should be noted that some commenters discuss “vertical” operation as the ability to communicate with command staff. This is obviously a distinct notion of verticality in interoperable communications.

¹⁷ SAFECOM *Grant Template: Roadmap to Beneficial Use Critical Plans* at 3 (March 31, 2005) (herein, “*SAFECOM Grant Template*”); William L. Pessemer, TOP PRIORITY: A Fire Service Guide to Interoperable Communications at 3 (The International Association of Fire Chiefs, 2006) (herein, “*Fire Service Top Priority*”) (available at <http://www.interoperability.virginia.gov/pdfs/FireService-InteropHandbook.pdf>).

¹⁸ 47 C.F.R. § 90.7; SAFECOM *Grant Template*, Note 17 *supra*, at 3; *Fire Service Top Priority*, Note 17 *supra*, at 3.

¹⁹ PL 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004.

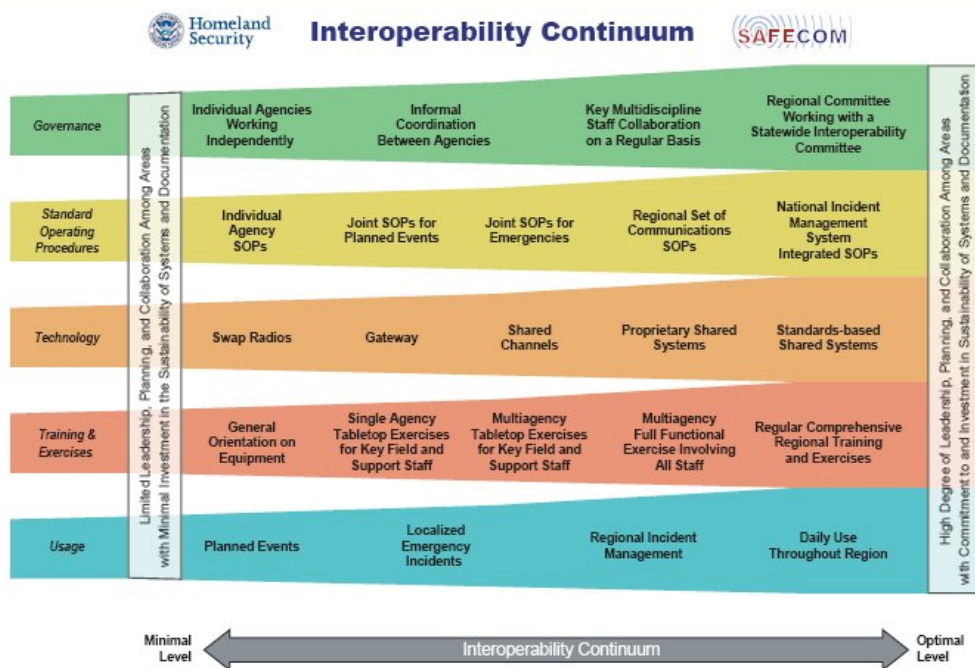
²⁰ United States Government Accountability Office, *FIRST RESPONDERS: Much Work Remains to Improve Communications Interoperability* (April 2007) (herein, “*GAO April 2007 Report*”) (available at <http://www.gao.gov/new.items/d07301.pdf>); SAFECOM *Grant Template*, Note 17 *supra*.

sixth characteristic: the ability to rely on accepted standards which promote and certify interoperable communications capability.²¹

B. Problems Flowing From Interoperability Failures

Notably, implementation of the family of interoperability characteristics is a matter of degree rather than a binary matter. This insight is well reflected in SAFECOM’s widely cited “Interoperability Continuum” chart (reproduced in Figure 1 below). The SAFECOM chart carves out five dimensions of interoperability and then illustrates progress – ranging from minimal to optimal – for each of these dimensions. A helpful aspect of this chart is that it visually underscores the connection between “people problems” (e.g., governance models and the development of coordinated operating procedures) and the adoption of optimal technology solutions. For example, absent an agreed upon set of standard operating procedures between agencies, available technological solutions will remain undeployed because of uncertainty as to how such resources would be used in responding to an incident.

Figure 1: SAFECOM Interoperability Continuum



This paper works from the proposition that interoperability problems remain a significant challenge for public safety responders. Many government initiatives,²² analyses,²³ and academic

²¹ This sixth characteristic is implicit in SAFECOM’s strong push toward Project 25 systems. While few commentators question the importance of standards in the area, some have questioned whether Project 25 should be the widely accepted standard. See, e.g., Dale Hatfield and Philip Weiser, *Toward a Next Generation Network for Public Safety Communications* at 15-16 (Silicon Flatirons Program May 2007) (herein, “*Silicon Flatirons May 2007 Report*,”) available at http://www.silicon-flatirons.org/conferences/Hatfield_Weiser_PublicSafetyCommunications.pdf. In the interest of disclosure, one of us – Brad Bernthal – assisted in drafting portions of this report.

²² For a list of initiatives providing federal support, see, e.g., SAFECOM *Grant Guidance* page (available at <http://www.safecomprogram.gov/SAFECOM/grant/default.htm>).

papers²⁴ have highlighted the fact that interoperability remains a formidable problem in public safety. Over the past decade, high profile disasters and incidents – including the shootings at Columbine High School on April 20, 1999, the events surrounding terrorist attacks in New York City on September 11, 2001, and the response to Hurricane Katrina in the Gulf region in August and September of 2005 – have generated numerous after-action assessments and reports identifying a lack of communications interoperability as compromising emergency response and costing lives.²⁵

Problems engendered by interoperability failures can be sorted into three general categories: (i) operational limitations, (ii) spectrum scarcity and unsatisfactory network capabilities, and (iii) expensive communication systems that are not cost-effective. Overall, “[the United States has] an extraordinarily balkanized system that generally lacks the ability to access and use the proliferating sources of electronic information held by other public and private organizations that can facilitate speedy and effective emergency response.”²⁶ When considering the *status quo* of public safety communications, it is clear that agencies too often continue to surrender *capability and value* in exchange for *control and comfort* in their communications systems. This is an ill-advised exchange, however, as explained in Part II below, close analysis makes one sympathetic to the many obstacles which must be navigated in order to achieve interoperability.

Operational limitations flow from incomplete or confused situational awareness where first responders cannot adequately communicate across diverse responding agencies. One way to conceptualize this is that public safety agencies with limited interoperability fail to realize what economists refer to as network externalities. Network externalities (or “network effects”) reflect the concept that “the value of the network to *each* use increases or decreases, respectively, with every addition or subtraction of *other* users to the network.”²⁷

In the public safety context, technological enablers and protocols which facilitate sharing *should* allow agencies to benefit by adding users and envisioning public safety as a network of networks.²⁸ For example, situational awareness should be enhanced as more nodes are available

²³ See, e.g., GAO April 2007 Report, Note 20 *supra*; June 8, 2005 CRS Report, Note 15 *supra*, at 18-22 (summarizing policy accomplishments).

²⁴ See, e.g., public safety communications articles in Volume 59, Issue 2 of the Federal Communications Bar Journal (available at <http://www.law.indiana.edu/fclj/pubs/v59no3.html>), including Philip J. Weiser, *Communicating During Emergencies: Toward Interoperability and Effective Information Management* (Vol. 59, Issue 2 Federal Communications Bar Journal 547) (March 2007); Jon Peha, *Fundamental Reform in Public Safety Communications Policy* (Vol. 59, Issue 2, Federal Communications Bar Journal 517) (March 2007); and Jerry Brito, *Sending Out an S.O.S.: Public Safety Communications Interoperability as a Collective Action Problem* (Vol. 59, Issue 2 Federal Communications Bar Journal 457) (March 2007).

²⁵ See, e.g., 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*, at 173, 178 (February 15, 2006) (<http://www.c-span.org/pdf/katrinareport.pdf>); The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* at pp. 293, 397 (Official Government Edition, Washington, D.C. 2004) (available at <http://www.9-11commission.gov/report/911Report.pdf>). For an examination following Hurricane Katrina, see, Philip Weiser, Dale Hatfield and Brad Bernthal, *Toward A Next Generation Architecture For Public Safety Communications* (2006) (available at http://papers.ssm.com/sol3/papers.cfm?abstract_id=903151).

²⁶ Carl Kent Ervin and David Aylward, *Next Generation Inter-organizational Emergency Communications: Making Tangible Progress While Broader Efforts Continue*, at 3, 7 (The Aspen Institute 2006) (herein, “*Aspen 2006 Emergency Communications*,” available at http://www.aspeninstitute.org/atf/cf/%7BDEB6F227-659B-4EC8-8F84-8DF23CA704F5%7D/Homeland_InteroperabilityReport.pdf).

²⁷ Jonathan Nuechterlein and Philip Weiser, *Digital Crossroads: American Telecommunications Policy in the Internet Age* at pp. 4-5 (MIT Press 2005).

²⁸ See Jon Peha, *How America’s Fragmented Approach to Public Safety Wastes Money and Spectrum*, 14, presented at 33rd Telecommunications Policy Research Conference (September 2005) (herein, “Peha”) (http://web.si.umich.edu/prc/papers/2005/438/Peha_Public_Safety_Communications_TPRC_2005.pdf) (“In an earlier age, the

to collect information, more points are available to process and transmit data, and resources can be pooled. To be sure, proper mechanisms and protocols are required in order to capture positive network effects. For example, as a recent report observes, the goal of interoperability is *not* “to communicate with any other individual at any time—a capability that could overwhelm the communications infrastructure and would likely impede effective communication and response time.”²⁹ But where proper mechanisms are implemented to authenticate and control communications, an overarching ambition of public safety agencies should be to become a network of networks in order to better capture network effects available from utilizing distributed intelligence.³⁰

Unfortunately, non-interoperable systems which fail to capture networks effects suffer as critical information fails to be collected, shared, and assimilated across responders. One of the starkest illustrations of this occurred during the 9-11 response, when “[c]ommand and control decisions were affected by the lack of knowledge.”³¹ One fire chief involved in 9-11 noted that people watching on TV had better information concerning events high in the tower than responders did. As a fire chief relayed to the 9/11 Commission: “One of the most critical things in a major operation like this is to have information. We didn’t have a lot of information coming in. We didn’t receive any reports of what was seen from the [NYPD] helicopters.” As a result, risks assessments and evacuation orders concerning collapse of the North tower were compromised. A similar failure to constructively harness information from distributed sources retarded response efforts in Hurricane Katrina. “DoD lacked an information sharing protocol that would have enhanced joint situational awareness and communications between all military components.”³²

A second unfortunate consequence of limited interoperability concerns scarce spectrum availability and unsatisfactory network capabilities. Current public safety spectrum assignments are typically treated as agency-specific stovepipes rather than inter-agency channels that can be pooled and used on an as-needed basis. “[T]he Federal Communications Commission has traditionally licensed private land mobile radio systems, including those used by public safety, on a local, jurisdiction-by-jurisdiction, site-by-site basis.”³³ One result of stove-pipe spectrum management is wasted spectrum.³⁴

advantages of fragmentation may have been outweighed by the advantage of allowing each municipality complete freedom to adjust its strategy to match local needs and resources. However, this is not the case today . . .”).

²⁹ *GAO April 2007 Report*, Note 20 *supra*, at 5.

³⁰ For a helpful discussion of how various types of channels – command and control, operational control, talk and mutual assistance, etc. – are used to enable interoperability *without* allowing each node on a network to freely talk to another, see Gerald Faulhaber, *Solving the Interoperability Problem: Are We On the Same Channel?*, at 496-97 (Vol. 59, Issue 2 Federal Communications Bar Journal) (March 2007) (herein, “Faulhaber,” available at <http://www.law.indiana.edu/fclj/pubs/v59/no3/8-Faulhaber.pdf>).

³¹ 9/11 Commission at 298.

³² *Katrina report – A Failure of Initiative*, Note 25 *supra*, at p. 4. It bears mention that interoperability issues were only part of communications problems following Hurricane Katrina, where communications were knocked out to the point that *operability* was a fundamental problem, raising questions concerning communications reliability and survivability. See Philip Weiser, Dale Hatfield and Brad Bernthal, *Toward A Next Generation Architecture For Public Safety Communications*, at 3 (2006) (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=903151).

³³ See *Silicon Flatirons May 2007 Report*, Note 21 *supra*, at 14.

³⁴ Peha, Note 28 *supra*, at 9; Peter Cramton, Thomas Dombrowsky, Jeffrey Eisenach, Allan Ingraham & Hal Singer, *Improving Public Safety Communications: An Analysis of Alternative Approaches*, at 20-21 (Criterion Economics, February 2007) (herein, “Cramton *et. al.*”) It is important to note, however, that it is often underappreciated that notions of “spectrum efficiency” are difficult to define in the dispatch/group call environment of public safety as compared to the one-to-one communications environment associated with commercial cellular systems. While it is easier to make the case that conventional, non-trunked public safety systems waste spectrum (or are at least less efficient than commercial cellular systems), it is more contentious argument as to whether wide-area trunked public safety systems designed for one-to-many communications are necessarily wasteful or less efficient.

The upshot of wasted spectrum is that public safety agencies either need to do more with their existing spectrum, or alternatively, more spectrum may need to be allocated to public safety going forward. A recent analysis estimates that of the 99.7 MHz allocated for public safety use once the 700 MHz spectrum is vacated, only 17 MHz is widely used to support public safety.³⁵ This observation should be tempered by three factors: (i) 24 MHz from the 700 MHz auction will not be transitioned until 2009, (ii) 50 MHz of the “little-used” spectrum is at 4.9 GHz, often referred to as the public safety Wi-Fi band, and (iii) most of the little used public safety spectrum is relatively new (allocated since 1996). Nonetheless, difficulties in cross-jurisdictional coordination contribute to a striking disparity in users per MHz of spectrum when comparing the private and public sectors. Relatively conservative calculations indicate an estimated average of 73,929 public safety users per MHz of spectrum, as compared to an average of 1,063,495 users per MHz of spectrum in private sector Commercial Mobile Radio System systems. “[E]ven recognizing that there are differences between public safety and CMRS systems, CMRS systems are dramatically more efficient in their use of spectrum than public safety systems.”³⁶

Moreover, even on public safety frequencies that are used, agencies often under-use their frequencies with respect to the time dimension of spectrum use. Public safety communications tend to be bursty and short rather than continuous and lengthy, meaning that public safety’s dedicated channels often go lightly used.³⁷ This is exactly the type of intermittent use that is well-suited for trunked and pooled systems: the same number of users can be accommodated using fewer channels; or, alternatively, more users can be accommodated using the same number of channels.³⁸ While a large-scale emergency or disaster may present an instance in which all channels see heavy usage, pooled spectrum nonetheless presents certain advantages if it is well-managed between users since this facilitates interoperability and – presuming that traffic is prioritized – high priority users have a greater chance of successful communications where channels are pooled. Notably, while the stove-pipe approach causes spectrum waste, a common “solution” to interoperability challenges, patching radios through a gateway, actually exacerbates spectrum scarcity.³⁹ Patching has the “effect of creating one communications channel, but it consumes twice the bandwidth throughout a greater area than a normal channel.”⁴⁰

The third unfortunate consequence of limited interoperability is that it is not a cost-effective approach. Not surprisingly, piecemeal purchases of equipment and communications systems are expensive. “Efforts to secure funding for initiatives that cut across agencies and jurisdictions are undermined by the common practice of financing government functions on an agency-by-agency, jurisdiction-by-jurisdiction basis.”⁴¹ Moreover, an additional effect of

³⁵ Cramton *et. al.*, Note 34 *supra*, at 19.

³⁶ *Id.* at 30. Removing the 50 MHz at 4.9 GHz and 24 MHz not yet transitioned to public safety, a reasonable (and perhaps conservative) estimate of available public safety spectrum is 25.7 MHz serving approximately 1.9 million public safety users. This results in an average of 73,929 users per MHz of spectrum, as compared to an average of 1,063,495 users per MHz of spectrum in private sector CMRS systems.

³⁷ Nancy Jesuale, *Cognitive Radio Use Cases and Spectrum Policy Issues for Public Safety and State and Local Government*, at 97 (Int. J. Network Mgmt 2006; 16: 89–101) (2006) (available at <http://delivery.acm.org/10.1145/1130000/1124501/p89-jesuale.pdf?key1=1124501&key2=6409486811&coll=GUIDE&dl=GUIDE&CFID=31437345&CFTOKEN=91470982>).

³⁸ See Brad Bernthal, Timothy X. Brown, Dale N. Hatfield, Douglas C. Sicker, Peter A. Tenhula & Philip J. Weiser, *Trends and Precedents Favoring a Regulatory Embrace of Smart Radio Technologies*, at 11-12, IEEE INT’L SYMPOSIUM ON NEW FRONTIERS IN DYNAMIC SPECTRUM ACCESS NETWORKS, Apr. 17-20, 2007.

³⁹ Peha, Note 28 *supra*, at 9.

⁴⁰ *Id.* Indeed, this may actually understate spectral waste engendered by patching. For example, where three responders could share one channel but instead choose to operate on three separate channels, and they are patched together using a switch or gateway, then the net effect of wasting three times as much bandwidth.

⁴¹ National Governor’s Center for Best Practices, *Issue Brief: Strategies for States to Achieve Public Safety Wireless Interoperability*, at 5 (November 2006) (herein, “Governor’s Center *Strategies for Interoperability*,” available at

balkanized systems is that – while they permit tailoring to local needs – overall they require more network infrastructure. That is, it “costs far more to deploy many small systems than it does to deploy a few large one” since duplicative infrastructure such as antenna towers, base stations and repeaters are often required, even where wireless systems feature a small number of users.⁴² Common purchases – or at least more widespread adoption of common systems – would enable longer production runs that would be more cost-effective.⁴³ However, rather than economies of scale and purchasing power, today’s more common scenario is that “each agency [] absorbs its own technology acquisition and customization costs and results in incompatibility and rapidly outmoded technologies.”⁴⁴

Moreover, the capabilities of public safety networks look increasingly impoverished compared to those that commercial providers have developed.⁴⁵ Indeed, many systems are simply old: between 20-40 years old.⁴⁶ While individual agencies possess spectrum for an exclusive communications system, individual agencies seldom have the expertise or resources to build out a sophisticated modern network with which to use their spectrum. To be sure, public safety systems often deliver rapid voice call setup (crucial for “shoot/don’t shoot circumstances) and group calling, where all members of a talk group receive transmissions from all other members of a talk-group.⁴⁷ Additional functionalities of modern dispatch systems include the ability to dynamically adjust talk group membership, “talk-around” ability which enables units to communicate directly in the absence of infrastructure (like a walkie-talkie), and an ability to queue and prioritize call requests when all channels are busy. While critical pieces of public safety communications, however, significant pieces are missing.

Perhaps most importantly, several commentators have noted that public safety communications remain in a narrowband world while commercial “[t]hird generation (3G) systems on the other hand can seamlessly handle voice, data, image and video traffic, employ packet-oriented switching, and operate in wideband channels (e.g., 1.25 MHz) allowing high data rate transmission roughly comparable to the speeds achievable by early generation wireline DSL and cable modem services.”⁴⁸ Indeed, one commentator has flatly observed that public safety “authorities have two main priorities for improving and upgrading communications systems: interoperability and broadband capability.”⁴⁹ Other trends being developed by commercial services – such as seamless hand-off possibilities network convergence, and use of updateable and extensible software in devices instead of fixed hardware – are also unlikely to emerge in public safety systems so long as such networks fail to be coordinated on a large scale.

<http://www.nga.org/Files/pdf/0903INTEROP.pdf>). Indeed, opportunities to create a nation-wide public safety network capable of purchasing in bulk animated discussions surrounding the 700 MHz proceeding’s “D-Block.”

⁴² *Id.* at 9.

⁴³ *June 8, 2005 CRS Report*, Note 15 *supra*, at 5 (“The greater the number of communications devices using compatible frequencies, the greater are the opportunities for economies of scale in production, which in turn typically lowers the cost and final price on equipment.”).

⁴⁴ *Aspen 2006 Emergency Communications*, Note 26 *supra*, at 7.

⁴⁵ See generally Space & Advanced Communications Research Institute (SACRI), George Washington University, *White Paper on Emergency Communications*, (Online Journal of Space Communication, Issue No. 10, Spring 2006).

⁴⁶ Governor’s Center *Strategies for Interoperability*, Note 41 *supra*, at 4.

⁴⁷ See *Silicon Flatirons May 2007 Report*, Note 21 *supra*, at 9.

⁴⁸ *Id.* at 12; Jerry Brito, *Sending Out an S.O.S.: Public Safety Communications Interoperability as a Collective Action Problem*, pp. 462-63 (Vol. 59, Issue 2 Federal Communications Bar Journal) (March 2007) (herein, “Brito,” available at <http://www.law.indiana.edu/fclj/pubs/v59/no3/7-Brito.pdf>).

⁴⁹ Cramton *et. al.*, Note 34 *supra*, at 14.

II. FOUR “PEOPLE PROBLEMS” DEFINED: UNDERSTANDING WHY INTEROPERABILITY PROBLEMS ARE DIFFICULT TO RESOLVE

Calls for public safety interoperability reflect the insight that government, by deploying 21st Century networked solutions, can (and should) provide improved services more efficiently to citizens.⁵⁰ But since public safety radio’s early origins when the Detroit Police Department in 1921 experimented with communications applications, public safety has not been architected for cross-agency interoperability with respect to organization, spectrum or equipment.⁵¹ Not surprisingly, as a general matter, the agency form of organization is not easily amenable to collaborative governance strategies. As scholar Edward DeSeve has observed:

“At all levels of government, most departments and programs were established to address specific problems with defined boundaries. This has had the effect of creating ‘silos’ within and across governments. There has been relatively little incentive to work across boundaries and even less training in the knowledge, skills, and abilities that are required for this kind of effort.”⁵²

More specific to the interoperability context, 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 fifty thousand US public safety agencies towards a commonly accepted set of objectives.”⁵³ It should not be entirely surprising, then, that intensified interoperability policy initiatives since September 11, 2001, have not produced quick results. Indeed, public safety reports regularly acknowledge that interoperability progress has been slow.⁵⁴ It is telling that even policy-makers recognize that the prospects of a near-term fix are dismal. For example, the director of the Department of Homeland Security’s Office for Interoperability and Compatibility last year testified that he believed that a dramatic change in interoperability would not occur prior to 2009 and, indeed, under “perfect conditions” such a change in communications systems would take at least until 2011 or even 2016.⁵⁵

Drawing upon work analyzing the broader challenge of achieving collaborative networks between public entities not originally designed for a hyper-networked environment, four factors emerge to explain why public safety cross-jurisdictional efforts have met stiff resistance: (1) risk arising from cross-jurisdictional collaboration; (2) inter-jurisdictional trust shortcomings; (3) principal-agent issues arising from instances in which an agent’s incentives are not aligned with a

⁵⁰ See generally, Business of Government Magazine, *Forum: Collaborative Governance*, at 45-70 (IBM Center for the Business of Government, Spring 2007) (available at <http://www.businessofgovernment.org/pdfs/forum07.pdf>); *What State CIOs Need to Know* at 1; Center for Technology in Government, University at Albany, SUNY, *New Models of Collaboration: An Overview* (October 2004) (available at http://www.ctg.albany.edu/publications/reports/new_models_exec).

⁵¹ For an excellent discussion of the origins and technical development of public safety communications systems, see *Silicon Flatirons May 2007 Report*, Note 21 *supra*, at 4-10.

⁵² DeSeve, *supra* Note 6, at 47.

⁵³ Peha, Note 28 *supra*, at 2.

⁵⁴ See, e.g., GAO April 2007 Report, Note 20 *supra*, at 3 (generally critical of results of DHS program results at state level, stating that absent “a more strategic approach” that “progress by state and localities in improving interoperability is likely to be impeded.”); Faulhaber, Note 30 *supra*, at 494 (“apparently little progress has been made in achieving the goal of interoperability”); *Aspen 2006 Emergency Communications*, Note 26 *supra*, at iii (“although some progress has been made, unfortunately [interoperability] is far from being solved”); *We Need to Talk*, Note 14 *supra*, at 1 (“there still has been little progress” in improving interoperability and spectrum use issues).

⁵⁵ *House Democrats Criticize FCC, Administration on Public Safety Interoperability Efforts*, TR Daily (April 15, 2006); but see Department of Homeland Security, *Tactical Interoperable Communications Scorecards: Summary Report and Findings*, at iii (January 2007) (relatively upbeat report based on scorecard results which, DHS believes, indicate that urban/metropolitan areas “have come a long way in improving their tactical interoperable communications capabilities.”).

principal's objectives; and (4) collective action problems.⁵⁶ Each of these is addressed in turn below.

(i) **Risk Triggered by Cross-Jurisdictional Collaboration**

Public safety agencies must surrender at least some autonomy and, additionally, rely on the performance of other agencies in order to achieve meaningful levels of communications interoperability. “[P]eople do lose some control when they cooperate [in an interoperable system] and, other things being equal, will resist giving up that control without a fight.”⁵⁷ Accordingly, the goal of achieving cross-jurisdictional collaboration is invariably contingent upon overcoming new dimensions of uncertainty generated for first responder agencies which participate in the network. Compounding this challenge is the fact that where a “project is also innovative and complex, risk is dramatically multiplied.”⁵⁸

Conceptions of risk are a significant obstacle in collaborative governance efforts, including public safety interoperability efforts.⁵⁹ This stems in part from the fact that public sector entities, such as public safety responders, “need to be perceived as responsible and responsive service providers.”⁶⁰ In contrast to a private actor likely view risk through the prism of financial cost/benefit probabilities, public sector agencies are inclined to gauge risk in terms of cost/benefit probabilities related to public perceptions of failure and whether the agency will serve its citizens.⁶¹

In a paper canvassing 12 collaborative network case profiles, Lise Préfontaine distills six type of notable risks factors triggered by cross-jurisdictional collaboration. Three of the six risks may be said to be *internal* to a collaborative project: (i) *organizational risks*, such as an inadequate management strategy, lack of leadership, lack of expertise among members of the team, and insufficient technical competence; (ii) *relationship risks*, such as an absence or

⁵⁶ This paper's list of interoperability barriers joins a line of similar “key problems” or “critical factor” lists. What situates this one somewhat differently (and, hopefully, saves it from being gratuitous), is that discussion of the six factors highlighted in this paper draws upon the wider body of collaborative governance literature in understanding why interoperability is hard to achieve. For a representative (and valuable) list of “key problems” viewed through a public safety-specific prism, see, e.g., Governor's Center *Strategies for Interoperability*, Note 41 *supra*, at 4 (“public officials must continue to address” (i) incompatible and aging communications equipment; (ii) limited and fragmented funding; (iii) limited and fragmented planning; (iv) lack of coordination and cooperation; and (v) limited and fragmented radio spectrum).

⁵⁷ Philip J. Weiser, *Communicating During Emergencies: Toward Interoperability and Effective Information Management*, at 566 (Vol. 59, Issue 2 Federal Communications Bar Journal 547) (March 2007) (herein, “*Effective Information Management*,” available at <http://www.law.indiana.edu/fclj/pubs/v59/no3/10-Weiser.pdf>).

⁵⁸ Lise Préfontaine, *Risk Management in New Models of Collaboration*, at 1 (Centre Francophone D'Informatisation des Organizations 2003) (part of *New Models of Collaboration* study spearheaded by Center for Technology in Government at University at Albany, SUNY) (herein, “Préfontaine,” materials available at http://www.ctg.albany.edu/publications/online/new_models/essays/risk).

⁵⁹ Since the events of 9/11, the strong push for public safety interoperability has perhaps muffled public discussion of risks inherent in collaborative networks. Nonetheless, this does not obscure the fact that such risks are crucial to address and resolve in order to achieve interoperability. For example, public safety communications risks triggered by interoperability include security concerns (*viz.*, who should be permitted to join the system? how will authentication and credentialing work? how are “bad” guys prevented from accessing the system?), reliability concerns (*viz.*, can the agency pay its fair share or might it default? do other agencies have technical competence to contribute to the network?), and – at least where spectrum is pooled – concerns whether other agencies can be trusted to only use their fair share of bandwidth (*viz.*, will other agencies “play nice” in spectrum sharing or will they overwhelm the entire network? will the collaborative network be able to route priority traffic as appropriate/needed through quality of service measures?). Indeed, when considering the perspective of a public safety agency currently under-using spectrum, the risk of joining a collaborative network can be significant; while pooling of spectrum is *exactly* the right thing to do from a net efficiency perspective, an entity that only sporadically uses its spectrum faces the dual risks of losing autonomy *and* introducing all-busy times to its services. Accordingly, such an agency can be expected to perceive large risk disincentives concerning pooling arrangements with agencies that use spectrum more intensively.

⁶⁰ Préfontaine, Note 58 *supra*, at 7.

⁶¹ *Id.*

shortage of agreements defining the relationship between entities in the collaborative network; and (iii) *risks inherent to the project*, including the technological complexity of the project and potential resistance to change and refusal to adopt by the collaborative network's users. An additional three risk factors may be understood to be *external* to the project, including (iv) *political risks*, such as competing or shifting goals between cooperating organizations; (v) *technological risks*, such as quick obsolescence of the technology used in the collaborative network; and (vi) *socio-economic risks*, such as changes in citizen preferences and expectations.⁶² Each of these risk factors is salient to considerations triggered by public safety interoperability and, if not managed, serve to frustrate coordination efforts.

(ii) Lack of Trust Between Agencies

One significant factor which especially affects an agency's decision-making calculus is the degree of trust between entities involved in a cross-jurisdictional collaborative effort. Inter-agency relationships devoid of trust can emanate from rivalry and turf wars, however, even where managers act in good faith, trust still may be lacking. This is because "[n]etworks, by their very nature, are composed of multiple members with different organization-level goals, methods of operation and service, and cultures."⁶³ Accordingly, mistrust can be a rational response to the different cultural postures and service objectives between multiple agencies considering collaboration. Indeed, lack of inter-agency trust is often cited as a core human factor which outweighs technical obstacles among interoperability challenges. "While it may appear to be a technical issue, interoperability has more to do with establishing trust and buy-in among stakeholders."⁶⁴

As part of the same project in which Préfontaine analyzed risk factors in cross-jurisdictional collaboration, Sharon Dawes focused on aspects of trust.⁶⁵ Of note, Dawes identified three different types of trust between the agencies working toward collaborative networks: (i) *calculus-based trust*, which stems from information collected impersonally (such as trust based on research and the reputation of another person or entity); (ii) *identity-based trust*, which flows from repeated direct interactions among participants in a network; and (iii) *institution-based trust*, where trust is derived from safeguards such as formal agreements and contracts among cooperating entities, social norms, and organizational structures involved in the network collaboration. Overall, these three dimensions of trust are critically important when adversity hits the collaborative network effort. "Inevitably, when things go wrong or the unexpected happens, professional commitment to the vision and goals of the project is needed to find acceptable solutions and keep the work going."⁶⁶

(iii) Principal-agent Issues

A third significant barrier to public safety interoperability flows from principal-agent problems where a misalignment exists between an agent's incentives and a principal's objectives. The principal-agent problem assumes that enhanced cross-jurisdictional interoperability would be

⁶² *Id.* at 2-6.

⁶³ H. Brinton Milward and Keith Provan, Business of Government Magazine, *Essential Tasks for Network Managers*, at 57 (Spring 2007) (herein, "Milward and Provan," available at <http://www.businessofgovernment.org/pdfs/forum07.pdf>).

⁶⁴ Governor's Center *Strategies for Interoperability*, Note 41 *supra*, at 7.

⁶⁵ Sharon Dawes, *The Role of Trust in New Models of Collaboration*, at 1-2 (Center for Technology in Government at University at Albany, SUNY, 2003) (herein, "Dawes," part of *New Models of Collaboration* study, materials available at http://www.ctg.albany.edu/publications/online/new_models/essays/trust).

⁶⁶ *Id.*

in the best interest of the principal (here, the public safety entity) but considers that the interest of the agent (here, an individual employee) may not match the principal's objectives.

In public safety, it should not be surprising that the principal's goals do not automatically dovetail with the incentives of individual agent who acts on behalf of the principal. For example, a technical employee who works on the existing communications network – and may well play a role in system procurement – may be resistant to changing to a new and unfamiliar system over which she has less control and, instead, may prefer to working in a silo-based system where fewer items outside of her control can go awry. “[T]he adoption of new technologies . . . may clash with the self-interest of a local official who operates a public safety network and wants to continue doing what she knows well.”⁶⁷ Additionally, another incongruity between individual incentives and the objectives of a government agency emanates from the different skills required to effectively manage within an organization's hierarchy as compared to skills required to effectively manage within a collaborative network. “The tasks of network management are different from those of managers in hierarchy.” Again, it is not surprising that individuals who are comfortable with their existing management abilities within an agency hierarchy may resist a move to a collaborative network paradigm which introduces professional uncertainty and may not fit their skill set competencies.⁶⁸

(iv) Collective Action Problems

Like principal-agent difficulties, collective action problems emerge when analyzing misaligned incentives between actors involved in public safety. In the collective action context, the misalignment exists between the incentives of an individual agency to act (or not act) and the larger course of action required to achieve a public good.⁶⁹ Jerry Brito, tracking the work of economist Mancur Olston, explains collective actions problems as follows:

“The term ‘collective action’ refers to activities that, in order to be successful, require two or more persons or entities to coordinate their efforts. Collective action is therefore group action meant to further the interests of the group. A collective action problem is simply a situation in which the rational course of action for the individual members of the group does not coincide with the group-oriented course of action necessary to obtain the ‘collective good.’ As a student of the collective action problem has summarized, ‘individual rationality is not sufficient for collective rationality.’⁷⁰

Brito asserts that public safety interoperability is a “classic example” of collective action problems where significant incentives exist for public safety agencies to try and free ride on the efforts of others.⁷¹ This is because where collective action requires the involvement of a large numbers of public safety agencies – as can be the case in collaborative public safety networks – individual agency participants often “have insufficient incentive to assume the costs” of achieving the common objective.⁷² In some instances, usually in smaller groups, free rider problems are

⁶⁷ *Effective Information Management*, Note 57 *supra*, at 567.

⁶⁸ Indeed, underscoring how these skills are different, part of the suggested transition for individuals to an effective collaborative network requires that “training occur[] at several levels: (1) collaboration, (2) the power of technology, (3) strategic thinking across boundaries, (4) results orientation, (5) leadership, and (6) change management.” DeSeve, *supra* Note 6, at 52.

⁶⁹ Brito, Note 48 *supra*.

⁷⁰ See Brito, Note 48 *supra*, at 463 (internal citations omitted).

⁷¹ Brito, Note 48 *supra*, at 464.

⁷² *Id.*

surmounted where a champion emerges because the champion would be better off achieving the group's objective, even if it has to pay the full cost of achieving the group's objective.⁷³ In larger groups in the absence of a champion, however, overcoming the collective action problem typically requires compulsion or individual incentives.⁷⁴

An excellent illustration of public safety collective action problems surrounds the trade off between spectrum usage and network infrastructure. There is a relationship between the intelligence of devices in a network (*e.g.*, transmitter and receiver capabilities) and the efficient use of spectrum: the more capable (but expensive) the infrastructure and network devices is, the more spectral efficiency can be achieved.⁷⁵ Since spectrum is an increasingly scarce resource, the public at large is often well-served by efforts to achieve more efficient spectral usage via use of greater intelligence in networks.⁷⁶ Notably, greater intelligence in networks facilitates increased interoperability.

However, while the greater good is achieved this way, the incentives for individual public agencies are differently situated. Significantly, public safety agencies get their spectrum for "free."⁷⁷ Accordingly, individual public safety agencies do not fully internalize the costs of inefficient spectrum usage. Given the trade-off involved between network capabilities and spectrum usage, an individual public safety agency has significant incentive to underinvest in the network – yielding less intelligent systems less amenable to interoperability – and rely instead on using "free" spectrum inefficiently. "Because public safety agencies receive spectrum 'for free,' and thus do not face appropriate economic incentives to use it effectively, the FCC (and other policymakers) need to encourage efficient use through the adoption of appropriate policies."⁷⁸

PART III. THE ALASKA LAND MOBILE RADIO CASE STUDY

"We're trying to do something that is new and different. And bureaucracies tend not to do well at that . . . The toughest part of this whole project has been governance."

-- Michael Callahan, Chief Information Officer for State of Alaska⁷⁹

The Alaska Land Mobile Radio system's primary virtue is also its greatest vulnerability: sweeping ambition. Indeed, a progressive vision of public safety interoperability is featured in nearly every dimension of the system, including the amount of shared assets and spectrum, geographic coverage (especially considering difficult Alaskan topology), cost, extent of interoperability (*viz.*, incidents and day-to-day), federal entity participation, common technology standards, and participation in the network across vertical and horizontal governmental entities.⁸⁰ On each of these scores, ALMR is anything but modest; indeed, ALMR attempts to achieve public safety interoperability on what may be an unprecedented scale.

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ Cramton *et. al.*, Note 34 *supra*, at 33.

⁷⁶ Indeed this is a goal of SAFECOM: RF system "must be spectrally efficient to a minimum quantifiable degree" and goals of spectrum and network efficiency are part of the list of requirements. See Cramton *et. al.*, Note 34 *supra*, at 24 (citations omitted).

⁷⁷ *Id.* at 33.

⁷⁸ *Id.* at 24.

⁷⁹ Telephone Interview with Michael Callahan, Chief Information Officer, State of Alaska (former Project Manager for ALMR) (conducted August 15, 2007) (herein, "Callahan August 15, 2007 Interview").

⁸⁰ There are two notable limitations to ALMR's ambition: (1) ALMR does not seek to be a broadband, packet-based, Internet Protocol network; and (2) while expansive in geographic coverage, ALMR does not attempt to provide blanket coverage for the entire state. As indicated in Figure 3, *infra*, ALMR's primary coverage areas are portions of Alaska accessible by highways and railroads.

Twelve years after the idea originally took root, ALMR now presents a compelling case study among existing interoperability efforts.⁸¹ In terms of operational results, ALMR has achieved shared use of network infrastructure, spectrum pooling, improved operational coordination, and expanded public safety network coverage. While ALMR's operational achievements are notable, however, they only convey part of the story. Indeed, the Project's ability to endure and overcome "people problems" is as noteworthy as its operational achievements. ALMR's history is replete with risks, trust problems and misaligned incentives: to date, some of these issues have been adroitly addressed; others remain inadequately resolved. For example, ALMR has demonstrated skillful reduction of political and policy risk by obtaining spectrum sharing waivers from the NTIA and FCC, implemented a dual project manager structure which reduces organizational risk, and used training extensively to enhance identity-based trust. ALMR's missteps, however, include a failure to anticipate or adequately manage political risk associated with rivalrous State agencies concerning the Project, shortcomings in addressing relationship risks between ALMR and local users, and assumed technological risk associated with a technical standard, Project 25, which invites principal-agent problems associated with expensive products.

The ALMR case study in this Part III proceeds in three parts: Subsection A provides an overview of the Project's scope and operational achievements; Subsection B focuses on risk factors encountered by ALMR; and Subsection C analyzes other incentive-related issues. Significantly, it is too early to judge whether or not ALMR will emerge as a long-term collaborative network success. ALMR is very much at an inflection point: there remains uncertainty as to whether ALMR can establish a sustainable way to fund the system on an on-going basis and, relatedly, whether relationship risk with local users can be addressed in a way which generates local user commitment to ALMR.

⁸¹ Other notable interoperability efforts include: the Wireless Accelerated Responder Network ("WARN"), which features spectrum and network sharing in order to provide broadband data services to federal and non-federal users (see U.S. Department of Commerce, *Spectrum Policy for the 21st Century – The President's Spectrum Policy Initiative: A Public Safety Sharing Demonstration* (May 2007) (herein, "WARN Demonstration Report") (available at <http://www.ntia.doc.gov/reports/NTIAWARNReport.pdf>); Virginia's Statewide Communications Interoperability Plan ("SCIP"), which the Commonwealth of Virginia created in partnership with SAFECOM (case study available at <http://www.safecomprogram.gov/NR/rdonlyres/DD91CD2C-FD2E-4BBC-AFEA-E620B4BBB891/0/SCIPMethodologyv20FINAL.pdf>); CapWIN, a collaborative effort between the State of Maryland, the Commonwealth of Virginia and the District of Columbia to "develop an interoperable first responder data communication and information sharing network" (see Governor's Center *Strategies for Interoperability*, Note 41 *supra*, at 3; interoperability efforts in Delaware, where the state system has been accepted in all counties and "is now in use by every police department, fire company, and EMCS unit" as well as other agencies (see Faulhaber, Note 30 *supra*, at 506-509); efforts toward achieving interoperability in Oregon through the Oregon State Interoperability Executive Council (see *Public Safety Communications Interoperability: Inventory and Analysis Report* (January 2005) (available at http://www.oregon.gov/SIEC/docs/SIEC_Publications/Inventory_and_Analysis_for_Oregon.pdf)); the Utah Communications Agency Network (UCAN) network (see web-site at <http://www.ucan800.org/>; U.S. Department of Justice and U.S. Department of Homeland Security SAFECOM Program, *2006 National Interoperability Summit Proceedings*, at 12, Prepared by SEARCH The National Consortium for Justice Information and Statistics (May 24-25, 2006) (available at <http://www.search.org/files/pdf/2006InteropSummitProceedings.pdf>); and the Central Nebraska Regional Interoperability Network (on-line PowerPoint overview available at http://www.naco.org/Content/ContentGroups/Programs_and_Projects/Information_Technology1/Summit/2007/DarrinLewis_TimLo_wenstein_NeilMiller.pdf). For a helpful case study of a non-public safety collaborative network (the New York State Geographic Information System), see Ophelia Englene and Sharon Dawes, *New Models of Collaboration: New York State GIS Coordination Program* (2003) (part of *New Models of Collaboration* study spearheaded by Center for New Technology in Government at University at Albany, SUNY, materials available at http://www.ctg.albany.edu/publications/reports/new_models/new_models.pdf).

A. Overview: ALMR Is a Highly Ambitious Project

ALMR Background

Geographic characteristics of Alaska – an area nearly one-fifth the size of the lower 48 states with topographical challenges including sometimes impassable terrain – inherently present significant communications coverage challenges for Alaska’s public safety first responders. Alaska’s vast and relatively sparsely populated area, however, simultaneously presents unique opportunities for first responders to share often thinly spread resources in order to improve coverage via collaboration.

The ALMR idea congealed in 1995. Responding in part to the prospect of National Telecommunications and Information Administration (“NTIA”) narrow banding mandates for federal users, the network’s original purpose was largely to integrate federal user radio communications in Alaska.⁸² As a general matter, the extent of federal efforts to be an essential part of ALMR is notable, insofar as federal agencies have otherwise struggled to serve as interoperability models.⁸³ Soon after the ALMR idea was created, an Alaska State Department of Public Safety study group recommended that, in connection with updating the State of Alaska’s Telecommunication’s Plan, that the State should consider a strategy which would avoid “doing the stovepipe thing all over again,” whereby each responder agency had its own dedicated spectrum and parochial communications system.⁸⁴ Support for the ALMR’s cross-jurisdictional collaboration effort was further galvanized by the 1996 Miller’s Ranch Fire, which burned 37,366 acres in Alaska over a two week period in early June 2006, as well as other natural and national disasters.⁸⁵ At the same time, it was recognized that many State agencies’ radio systems were nearing the end of their useful life. By 1997, it was clear that ALMR’s purpose would be broader than just connecting federal users.⁸⁶

ALMR swings – at least metaphorically – for the collaborative network fences insofar as public safety interoperability goes. Notably, the ALMR Executive Council Interoperability Plan provides for three types of public safety interoperability: (i) day to day interoperability;

⁸² Telephone Interview with Douglas Robinson, Communications Superintendent, Municipal Light and Power (Anchorage, Alaska), former member of ALMR Executive Council (conducted August 16, 2007) (herein, “Robinson August 16, 2007 Interview”).

⁸³ See, e.g., Donny Jackson, Mobile Radio Technology, *Feds See That Interoperable Communications Is Easier Said Than Done* (March 29, 2007) (available at http://mrtmag.com/iwce/commentary/interoperability_government_iwn_032907/) (discussing fracturing of federal agency interoperability efforts in the Integrated Wireless Network (IWN)); First Response Coalition, *Interoperability Innovation: State Best Practices & Models for First Responder Communications*, at 5 (March 2007) (noting the “ongoing but uneven federal interoperability response” which has spurred states to take the interoperability lead).

⁸⁴ Telephone Interview with Del Smith, Operations Manager, Alaska Land Mobile Radio (conducted August 16, 2007) (Herein, “Smith August 16, 2007 Interview”) (Mr. Smith was part of the DPS group which made this recommendation).

⁸⁵ Letter of Major General Craig Campbell on behalf of the Department of Military and Veterans Affairs in response to ALMR Audit, at 1 (herein, “DMVA Audit Response,” dated December 21, 2005) (available as Exhibit to 2005 Audit). For information on the Miller’s Ranch fire, see the DMVA web-site, *Miller’s Reach, Fire Hazard Mitigation Grant Program* (available at <http://www.ak-prepared.com/plans/mitigation/mrfire.htm>).

⁸⁶ *Audit Report on Alaska Land Mobile Radio Project*, at 5 (Audit Control Number 09-30021-06 September 21, 2005) (herein, “2005 ALMR Audit Report,” available at <http://www.legaudit.state.ak.us/pages/audits/2006/pdf/30021rpt.pdf>). Formal documentation of various ALMR-related collaborative initiatives ensued. In 2001, for example, as ALMR pursued a P25 system, a memorandum of understanding was executed to “‘move forward with implementation of a cooperative solution’ that meets the needs of the federal, state and local agencies for ‘mutual aid, disaster response and crisis management as well as day-to-day operations.’” *Id.* at 5-6, quoting *Memorandum of Understanding Between State of Alaska, Alaska Municipal League, Department of Defense Alaska Command, and Federal Executive Association of Alaska* (MOU dated April 4, 2001). Two years later, the Executive Council’s Charter was again revised to reflect on-going cooperative efforts, providing that the ALMR project “represents a consortium approach to governance of the implementation, operation, maintenance and management of the shared trunked and conventional land mobile radio infrastructure.” Alaska Land Mobile Radio Executive Council, *Charter For the Alaska-Wide Land Mobile Radio Executive Council*, Article I (April 10, 2003) (available at <http://www.ak-prepared.com/almr/pdf/ALMR%20Executive%20Council%20Charter%20-%20April%2010.%202003.pdf>) (emphasis added).

(ii) mutual aid and disaster response interoperability; and (iii) task force interoperability.⁸⁷ The first type – day-to-day interoperability – coordinates relatively routine operations such as the pursuit of a suspect across jurisdictional boundaries where “an agency is required to talk to another because one or more agencies have crossed over into another agencies [sic] jurisdiction and communication is required between agencies to coordinate and execute an operation.”⁸⁸ The second type – mutual aid and disaster response/coordination interoperability – involves tactical communications where one agency faces a major incident or disaster requiring greater responder resources than the agency possesses, such as plane crash, terrorist attack, or earthquake.⁸⁹ And the third type – task force interoperability – is required following major incidents or in connection with major events. Task force interoperability is utilized where cross-agency collaboration (both horizontal and vertical) is required for an extended period of time. For example, communications for a major event (e.g., the Olympics) or following a large disaster (e.g., a terrorist attack) may require task force interoperability.⁹⁰

Spectrum and Infrastructure Sharing

ALMR achieves interoperability through a range of sharing methods, however, the most notable and significant aspect is ALMR’s initiative to share both spectrum and infrastructure. ALMR’s pooling of spectrum is particularly significant as it enables federal users to use frequencies assigned by the FCC to State agencies and, concomitantly, permits non-federal users to use frequencies assigned by the NTIA to federal users. This type of sharing is prohibited absent a regulatory exception so, in this respect, ALMR is “precedent-setting.”⁹¹

ALMR uses two swaths of frequencies located in the VHF segment of the electromagnetic spectrum: (i) 1.5 MHz from the non-federal public safety pool between 154.65 -156.24 MHz (controlled by the FCC); and (ii) another 1.5 MHz from the federal spectrum located between 138 – 144 MHz (controlled by the NTIA).⁹² Figure 2 below shows the location of these public safety bands in the VHF spectrum band.⁹³ The significant bands in ALMR are the two middle bands (shaded blue), with the lower band representing shared federal spectrum and the non-federal shared spectrum shown in the upper band.

⁸⁷ Alaska Land Mobile Radio Executive Council, *Interoperability Plan for the State of Alaska (Region 2)*, at 7 (April 2003) (herein, “April 2003 Interoperability Plan,” available at www.apcointl.org/frequency/siec/documents/alaska.pdf).

⁸⁸ *Id.* at 7. The logical organization of the ALMR system is designed to facilitate day-to-day operations using a simple yet effective hierarchical scheme. The state is divided up into six zones collectively covering all of the populated cities and towns within the state. Each zone has 15 talk groups controlled at the municipal level.⁸⁸ The 15 talk groups are then subdivided and assigned to individual departments for use. Access to other departments is policy restricted to prevent unintended communication across the administrative boundary during day-to-day usage.

⁸⁹ *Id.*

⁹⁰ *Id.* at 7-8.

⁹¹ See Robert Howk, Alaska Journal of Commerce, *New Emergency Radio System Is Nation’s First* (October 20, 2003) (quoting Program Manager Tim Woodall).

⁹² FCC Waiver Order, *supra* Note 12, at 4.

⁹³ See also GAO April 2007 Report, Note 20 *supra*, at 7 (providing a more detailed diagram of all public safety bands in the VHF and UHF bands).

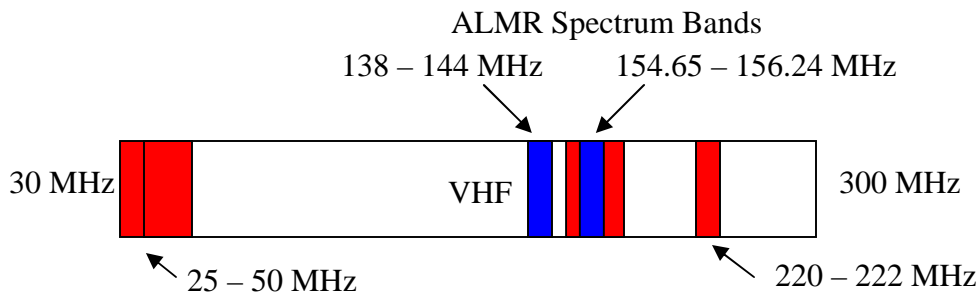


Figure 2: VHF Public Safety Bands

Agencies using ALMR utilize the lower federal band, 138 – 144 MHz, for all mobile and portable handset communications.⁹⁴ This is an elegant method to achieve interoperability: because it allows all handsets in Alaska to operate on the same 138 – 144 MHz frequencies, both federal and non-federal users can participate in any talk group without occupying additional spectral resources or requiring additional network equipment.⁹⁵ Meanwhile, on the upper non-federal 154.65 – 156.24 MHz band, high power base stations and repeaters are used to carry the traffic of low power mobile handsets throughout the network. Notably, absent spectrum sharing, LMR systems would have to dedicate spectrum resources for inter-base station communications (cutting the number of possible talk groups as much as half). By pooling resources together, Alaska agencies are able to maximize the number of talk groups for their size of given spectrum bands.

In addition to spectrum, fixed infrastructure – which serves as the backbone transport for all services – is critical to any large radio communications system. When complete, the ALMR fixed infrastructure will be comprised of an estimated 97 sites; as of July 2007, 67 of these sites are operational.⁹⁶ Significantly, where possible, ALMR leveraged existing sites from the pre-existing structural communications backbone of the State of Alaska, the State Telecommunications System (SATS). SATS is a microwave-based system designed to help provide two-way communications for public safety as well as additional data processing and telephony links.⁹⁷ In addition to using SATS’ backbone capabilities, ALMR has collocated with SATS sites for roughly 2/3 of the ALMR fixed infrastructure.⁹⁸ For these sites, the ALMR plan called for the State of Alaska to pay for site preparation work while the DoD would buy and install necessary equipment.⁹⁹ The map image below depicts fixed infrastructure sites supporting the ALMR.

⁹⁴ The difference between mobile and portable handsets is the size, power and range capabilities of the device. A mobile handset is small and can be carried by a person (e.g. radio carried on the belt of a police officer) because of its small size it has the lowest operating power and therefore has a line of sight range between 2 and 5 miles. A portable radio is larger and is portable in a vehicle (e.g. the radio in a patrol car) the increased power available enables a portable handset to have a line of sight range up to about 20 miles.

⁹⁵ ALMR’s systems are typically “trunked” whereby a common pool of channels support a large user base with electronically controlled access to the channels. Trunked systems “promote economic efficiency because, for a given quality of service, more traffic can be handled over the same number of channels (or, alternatively, the same amount of traffic can be handled over fewer channels). See Brad Bernthal, Timothy X. Brown, Dale N. Hatfield, Douglas C. Sicker, Peter A. Tenhula & Philip J. Weiser, *Trends and Precedents Favoring a Regulatory Embrace of Smart Radio Technologies*, at 12, IEEE INT’L SYMPOSIUM ON NEW FRONTIERS IN DYNAMIC SPECTRUM ACCESS NETWORKS, Apr. 17-20, 2007.

⁹⁶ ALMR, User Council Meeting Minutes (July 11, 2007) (available at http://www.ak-prepared.com/almr/user_council.htm).

⁹⁷ 2005 ALMR Audit Report, Note 86 *supra*, at 3, 14 (concerning background of ALMR project).

⁹⁸ *Id.* at 6.

⁹⁹ *Id.* In practice, this has met with mixed success; at times, DoD has had to pick up costs originally marked for the State. *Id.* at 9.



Figure 3: Fixed Infrastructure sites for the ALMR system¹⁰⁰

The disproportionate density of fixed sites in southeastern Alaska (as opposed to other areas of the Alaska) reflects that ALMR does not attempt to provide blanket coverage for the entire state; rather, ALMR’s main footprint is along areas of Alaska accessible by highways and railroads.¹⁰¹ In lieu of a full state build-out, a transportable capability has been developed which features four “skids.”¹⁰² Each skid is a rapidly transportable system which provides a P25 trunk site, plus additional voice and data services.

Reviews of ALMR’s Operational Capabilities

Reported initial reviews of ALMR’s operational capabilities have ranged from generally favorable to strongly enthusiastic.¹⁰³ Training exercises, in particular, have underscored the system’s merit. For example, ALMR received “rave reviews” following a 2005 military exercise

¹⁰⁰ 2005 ALMR Audit Report, Note 86 *supra*.

¹⁰¹ An earlier vision of ALMR sought to provide greater coverage but this plan was scaled back in 2003-04. Testimony of Major General Craig Campbell, Alaska State Senate Finance Committee Minutes, at 2 (March 23, 2005) (herein, “MG Campbell Testimony March 23, 2005,” available at <http://www.legis.state.ak.us/pdf/24/M/SFIN2005-03-230905.PDF>).

¹⁰² “Alaska Land Mobile Radio System is a template for U.S. Homeland Security/Homeland Defense Communications. Stephen Larson, PROJ MGR, Defense Communications & Army Transmissions Systems (PM DCATS), Release No: 05-12-01 (available at <http://www.eis.army.mil/dcats/n-05-12-01.html>).

¹⁰³ Donny Jackson, *Trailblazers* (MRT Magazine) (April 1, 2006) (available at http://mrtmag.com/mag/radio_trailblazers/index.html) (last checked July 19, 2006). Additionally, in a recent DHS interoperability review, the Anchorage area fared well, with DHS commenting on ALMR and noting that during the exercise “the participants effectively used their interoperable communications assets across all levels of government and types of support disciplines[.]” Department of Homeland Security, *Tactical Interoperable Communications Scorecards Summary Report and Findings*, (January 2007). Additionally, as of August 2007, results of an ALMR user survey are being processed, which will provide further insight into ALMR user experiences. See Smith August 16, 2007 Interview, Note 84 *supra*.

in which state and local first responders participated with federal agencies including the FBI and the Federal Emergency Management Agency.¹⁰⁴ Moreover, interviews with various officials who have worked closely with the Program indicated that the system “works very well” and that – aside from general reluctance by some users to learn a new radio system and selected coverage gaps – most users have found value in ALMR.¹⁰⁵ The ALMR’s Operational Manager, Del Smith, a 30 year veteran of public safety, observed that “it is an amazing system – I’m blown away by the quality.”¹⁰⁶ Perhaps the best indication of ALMR’s utility is user migration to the system: in addition to day-to-day use by the DoD at Elmendorf and Eielson Air Force Bases, notable State and local entities that now regularly use ALMR include the State Department of Public Safety (in particular, the Alaska State Troopers), the Alaska Department of Transportation and Public Facilities, and responder agencies in cities such as Fairbanks and Valdez.¹⁰⁷

B. ALMR’s Ability to Endure and Overcome People Problems – Including Risk Factors – Is As Noteworthy as Its Operational Achievements

Development of a collaborative network inevitably faces significant risk factors. The ALMR project is not immune. Analyzed below are five of the risk factors identified in Part II, including risks *internal* to the collaborative project (*viz.*, *relationship risk*, *inherent project risk*, and *organizational risk*) and risks external to the Project (*viz.*, *political* (including policy) *risk* and *technological risk*).¹⁰⁸ Given its large scale and wide breadth of ambition, it is unsurprising that ALMR has encountered challenges relating to several risk factors over the past 12 years. Indeed, ALMR’s history provides a rich case study replete with “people problems” and a collaborative network’s strategies to address such issues. Each of these factors is addressed in the ALMR context in turn below.

(i) Relationship Risk: ALMR’s 800 Pound Gorilla

Relationship risks arise where agreements between entities are absent or such agreements fail to adequately specify the respective roles and responsibilities of the members in a collaborative network. Indeed, relationship risks between the ALMR system and local agencies in Alaska are the 800 pound gorilla that the Project must address in the near term (*viz.*, the next 6-12 months).¹⁰⁹ Indeed, ALMR is at an inflection point: while the system is notable for its success in

¹⁰⁴ Donny Jackson, *Trailblazers* (MRT Magazine) (April 1, 2006) (available at http://mrtmag.com/mag/radio_trailblazers/index.html) (last checked July 19, 2006); *see also* Stephen Larsen, PM DCATS News, “Alaska Land Mobile Radio System is a template for U.S. Homeland Security/Homeland Defense Communications,” Release Number 05-12-01 (citing ALMR as a model for inter-agency cooperative networks).

¹⁰⁵ Callahan August 15, 2007 Interview, Note 79 *supra*; Robinson August 16, 2007 Interview, Note 82 *supra*; Telephone Interview with Michael O’Hare, Department of Military and Veterans Affairs (conducted August 15, 2007) (noting need for some additional repeaters to cover gaps).

¹⁰⁶ Smith August 16, 2007 Interview, Note 84 *supra*.

¹⁰⁷ Robinson August 16, 2007 Interview, Note 82 *supra*. George R. Keeney, Valdez Fire Chief, has explained how the ALMR system has improved his department’s capability to communicate: “[Prior to the ALMR,] we had trouble talking to fire department personnel even one mile away from each other. When we went into building we lost communications. As a fire chief I had to worry about crews in fires and not being able to talk to command. Since the system has been turned on at the divide in Thompson Pass we now have communications that are great. I would like to tell you as of yesterday we checked the signals through our area and all the way to Anchorage and Fairbanks. We have almost full coverage and it is clear, even in Keystone Canyon. The majority of the area we can use even the hand held radios.” Talking Points, *Alaska Interoperable Communications*, Volume 2, Issue 3, April 2006 (available at <http://www.ak-prepared.com/almr/pdf/Newsletter%204-06.pdf>)

¹⁰⁸ Préfontaine, Note 58 *supra*, at 2-6. One risk factor – *socio-economic risk* – is omitted from this discussion. This is because, on this score, the “risk” of shifting vicissitudes of public opinion have generally been addressed by events beyond ALMR’s control, such as high profile incidents and disasters since 1995 which have reinforced the importance of first responder interoperability and, in general, enhanced support for the Project. That said, the 2005 state audit of ALMR (discussed in this section below) was far from flattering in its assessment of the State’s mishandling of the Project. Additional research may focus on how the Project dealt with *socio-economic risk* arising from this embarrassment.

¹⁰⁹ The time urgency largely relates to funding of the Project after the build-out and implementation are complete. To date, there has been political will sufficient to help complete build-out and implementation of the network. *See* State of Alaska FY2007

achieving collaborative network operational capabilities, it remains to be seen whether ALMR emerges as a sustainable initiative capable of maintaining a sizable percentage of Alaska’s local responders in the network fold. Fundamentally, current ALMR risks emanate from a failure to clearly define the nature of local agencies’ relationships with the Project.¹¹⁰ In particular, critical issues surround responsibility for ALMR’s on-going operational and management costs. “[T]he primary reservation that prospective local government users have about participating in the ALMR is costs – both the costs involved with acquiring new radio gear and the ongoing operational costs assessments they will be required to pay in the future.”¹¹¹

A 2005 review of ALMR by Alaska’s Legislative Auditor scorched the State’s handling of ALMR build-out and implementation project costs.¹¹² The audit found that the Project’s cost estimates were developed without adequate basis and, moreover, the auditor suspected that cost estimates were simply derived with an eye toward funds perceived to be available.¹¹³ For example, when fixed infrastructure cost bids from a contractor exceeded earlier estimates, the overall budget remained virtually unadjusted as the fixed infrastructure’s increase was simultaneously off-set by a similar decrease in radio costs.¹¹⁴ The audit looked upon this change with considerable skepticism. In addition, the failure to accurately *estimate* the build-out costs has been followed by shortcomings in tracking the Project’s *actual* build-out and implementation costs.¹¹⁵ As a result, inadequate records have frustrated the ability to clearly define expected operational costs for users going forward.¹¹⁶ “The lack of an accurate, workable project cost estimate, coupled with the lack of accumulating maintenance costs on a site-by-site basis, has limited the State’s project office from providing critical information to prospective users.”¹¹⁷ Until user costs are determined and local users commit to joining ALMR on an on-going basis, the Project faces a large relationship risk vis-à-vis local users.

Significantly, all current ALMR users are technically deemed “Beta” users since the ALMR build-out is not yet complete and certified for beneficial use.¹¹⁸ Accordingly, while operating under the Beta Period agreement, no user fees are collected.¹¹⁹ The “Beta” program is itself a meritorious strategy insofar as it effectively allows users to try out the ALMR system with minimal risk. Understandably, however, before signing on to an agreement to become a permanent (or at least long term) ALMR user, local users want to know what the cost will be before they decide to join ALMR. Of note is the fact that the City of Anchorage, citing in-building needs, recently decided to build out a new system which will not directly be part of the

Governor’s Operating Budget, *Department of Military and Veterans Affairs Alaska Statewide Emergency Communications Component Budget Summary*, p. 9 (2007) (available at http://www.gov.state.ak.us/omb/07_OMB/budget/DMVA/comp2781.pdf). It is unclear, however, whether there will be political appetite to continue funding levels that effectively subsidize the operational costs of non-State level agency users on the network.

¹¹⁰ ALMR, User Council Charter, Meeting Minutes, at 4 (January 4, 2006) (available at http://www.ak-prepared.com/almr/user_council.htm).

¹¹¹ 2005 ALMR Audit Report, Note 86 *supra*, at 24.

¹¹² See 2005 ALMR Audit Report, Note 86 *supra*, at 12.

¹¹³ *Id.* at 11-12 (cost “estimate raises questions as to its basis and underlying accuracy . . . [cost projections] were developed from actual and projected available funding”).

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 22-23.

¹¹⁶ Exacerbating this problem is that agencies failed to keep track of ALMR records when State departmental responsibility was transferred from the Department of Administration (“DoA”) to the Department of Military and Veteran’s Affairs (“DMVA”). *Id.* at 22-23 (with the move from DoA to DMVA, “copies of all documents related to the project should have been kept”).

¹¹⁷ See 2005 ALMR Audit Report, Note 86 *supra*, at 16.

¹¹⁸ Smith August 16, 2007 Interview, Note 84 *supra*.

¹¹⁹ Alaska Land Mobile Radio, “Beta Period” Membership Agreement, at Part IV(A) (draft dated December 8, 2004) (“The Member will pay no Activation Fee per radio and no Subscriber Fee during the Beta Period.”).

ALMR network and, instead, will rely on patching technology to achieve interoperability.¹²⁰ Anchorage believes that this approach will provide better in-building coverage without having to use additional equipment (e.g., bi-directional amplifiers). Other localities face similar architectural choices in replacing aged systems as the FCC's narrow-banding mandate set for 2013 approaches.¹²¹ As ALMR completes implementation and moves out of its Beta phase, local user buy-in is crucial: the extent of ALMR's achievement as a fully realized collaborative network hangs in the balance. Accordingly, relationship risks between the ALMR entity and local users present the network's greatest challenge today.

(ii) **Risks Inherent to the Project: Maintaining Command and Control**

Public safety networks must remain capable of supporting hierarchical command and – to a certain degree – resist certain flattening forces typical of 21st Century networks. “The function of public responder radio is to enable the Commander on the scene to maintain situational awareness, to control his or her operational resources, and to command other companies and agencies assisting at the scene.”¹²² Accordingly, ALMR's operational success requires that it not compromise command and control communications when responders arrive at an event or incident. To help accomplish this, mutual aid and disaster response are managed using the Incident Command System (“ICS”), which provides detailed instructions to follow for disaster response.¹²³ Specifically, ALMR's elegant spectrum sharing approach makes implementation of ICS processes orderly and user-friendly.

When an incident occurs, the Incident Command immediately appoints an incident commander to serve as a single source for direction.¹²⁴ At this point, the incident commander assumes full control of the ALMR resources as needed. Within the federal spectrum that is used for mobile handset communications, the ALMR network has three bands that support hierarchical command and control communications: low, middle, and high. The low band is for intra-jurisdiction control. For example, a police chief coordinating efforts within his jurisdiction will use this band to control police operation. The middle band is used for inter-jurisdiction coordination. For example, a neighboring fire department responding to help fight a fire can talk between agencies on this band. The top band is used for the ICS command and control. It is on this band that the incident commander will coordinate the efforts of the various federal, state and local agencies involved. While both the middle and top bands support inter-jurisdiction interoperability, the individual role fulfilled by each band differs slightly: the middle band is for day-to-day interoperability between agencies (e.g., fire departments responding to help a neighboring department fight a fire); meanwhile, the high band is available specifically available to meet the command and control needs of the ICS and incidents that are outside the scope of

¹²⁰ Department of Homeland Security, *Tactical Interoperable Communications Scorecards: Summary Report and Findings*, at B-5 (January 2007) (available at <http://www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf>).

¹²¹ See ALMR, *FCC Narrow-band Mandate Primer Impact and ALMR Compliance* (available at http://www.ak-prepared.com/almr/pdf/071107%20Meeting%20Attachments/20070618_Narrowband.pdf).

¹²² Faulhaber, Note 30 *supra*, at 494.

¹²³ ICS “is a disaster management tool based on a series of rational bureaucratic principles” which has become particularly important in view of “the federal government’s current initiative to make ICS the disaster operations law of the land in the form of the National Incident Management System (NIMS).” Dick Buck, Joseph Trainor, and Benigno Aguirre, *A Critical Evaluation of the Incident Command System*, at 1, 3 (Journal of Homeland Security and Emergency Management)(Vol. 3, Issue 3, 2006).

¹²⁴ Within ALMR, the incident Chain of Command follows the following jurisdictional rules: for a land based incident within the boundaries of the State of Alaska, the incident command falls under the direction of the Department of Public Safety, Alaska State Troopers; for water based incidents occurring in major waterways, bays, harbor areas and oceans, the US Department of Transportation, US Coast Guard, 17th Coast Guard District, has incident command authority; for airspace over Alaska, the Department of Defense, Alaska NORAD Region, has incident command authority. See April 2003 Interoperability Plan, Note 87 *supra*, at 5.

day-to-day operations.¹²⁵

Significantly, the use of a common command and control channel is ideal for incidents when ICS jurisdictions are crossed. For example, a hijacked airplane in-air is within the jurisdiction of the Air Force; however, jurisdiction over the incident transfers to the State Police once the plane touches down on a runway.¹²⁶ Prior to the ALMR common command channel, every agency would have to either change from the DOD command channel to the State Police command channel, or pick up a State Police reserve radio if their equipment was not interoperable with the State Police. A training exercise in Alaska looked at this scenario and the feedback was that it is “amazing how well this worked.”¹²⁷

(iii) **Organizational Risk: An Evolving Approach to Leadership**

Organizational risks faced by collaborative networks include leadership failure, inadequate management strategy, and lack of expertise among members of the team. A lynchpin of ALMR’s accomplishments has been a governance structure which permits leadership needed to address the Project’s primary challenges. The import of leadership is not itself surprising. Indeed, the public safety community is well acquainted with the importance of governance strategies which facilitate leadership in collaborative efforts.¹²⁸ “Governance offers a method for seeing beyond the individual agency, and breaking down regional and discipline and funding barriers.”¹²⁹ While the importance of governance structure is nothing new, however, what is notable about ALMR has been its ability to adjust its governance structure over time to address changing leadership needs.

When selecting a governance design for a collaborative network project, there are several alternatives. Figure 4 below shows three potential forms of network governance.

¹²⁵ Callahan August 15, 2007 Interview, Note 79 *supra*.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ U.S. Department of Justice and U.S. Department of Homeland Security SAFECOM Program, *2006 National Interoperability Summit Proceedings*, Prepared by SEARCH The National Consortium for Justice Information and Statistics, at 19-21 (May 24-25, 2006) (herein, “2006 National Interoperability Summit”) (available at <http://www.search.org/files/pdf/2006InteropSummitProceedings.pdf>) (“Why is governance critical to the success of the effort? The consensus of the focus groups: *Nothing else works without it.*”).

¹²⁹ *Id.* at 21.

Design Characteristics	Self-Governance	Lead Organization	Network Administrative Organization (NAO)
Structure	No administrative entity, participation in network management by all members	Administrative entity (and network manager) is a major network member/service provider	Distinct administrative entity set up to manage the network (not a "service provider")—manager is hired
Optimal number of members	Few	Many	Many
Decision making	Decentralized	Centralized	Mixed
Advantages	Participation, commitment by members, ease of forming	Efficiency, clear network direction	Efficiency of day-to-day management, strategic involvement by key members, sustainable
Problems	Inefficient—frequent meetings, difficulty reaching consensus, no network "face"	Domination by lead organization, lack of commitment by members	Perception of hierarchy, cost of operation, complex administration

Figure 4: Alternative Forms of Network Governance – the Management of Design¹³⁰

At ALMR’s inception, a relatively centralized leadership structure was implemented during stages when the Project’s primary challenges involved securing buy-in from key stakeholders, obtaining funding, and contracting to build-out the network. This initial governance structure – utilized in various forms from 1995-2005 – in many respects reflected the “Lead Organization” model (delineated in Figure 4 above) insofar as the major network members – especially DoD and the State – provided hands-on leadership and provided valuable human resources to execute key aspects of ALMR projects. Significantly, ALMR’s governance hierarchy was led by a strong Executive Council vested with the power to lead the Project.¹³¹

Centralized leadership in the Executive Council enabled key stakeholders – and, in particular, the DoD and the State – to serve as the Project’s “face” in championing the Project during its formative years. At the same time, while the Executive Council enjoyed centralized power, this power was split between four stakeholder co-chairs, including one representative each from Federal-DoD, Federal Non-DoD, State of Alaska, and the Alaska Municipal League.¹³² A strong, four-member Executive Council averted some of the inefficiencies that would have attended having an ungainly number of members; meanwhile, giving equal voting power to each stakeholder group helped mitigated the risk that one entity – viz., DoD – would simply commandeer the collaborative project at the expense of others. Notably, the co-equal member structure was an interesting determination since the Alaska Municipal League would, for the most part, not directly provide funding for the Project. This decision to include the Municipal League as a co-equal showed an understanding of the importance of local agency support to the Project and, moreover, opportunities for local agencies to secure federal grant funding for the Project going forward.

¹³⁰ Milward and Provan, Note 63 *supra*, at 61 (Spring 2007) (available at <http://www.businessofgovernment.org/pdfs/forum07.pdf>).

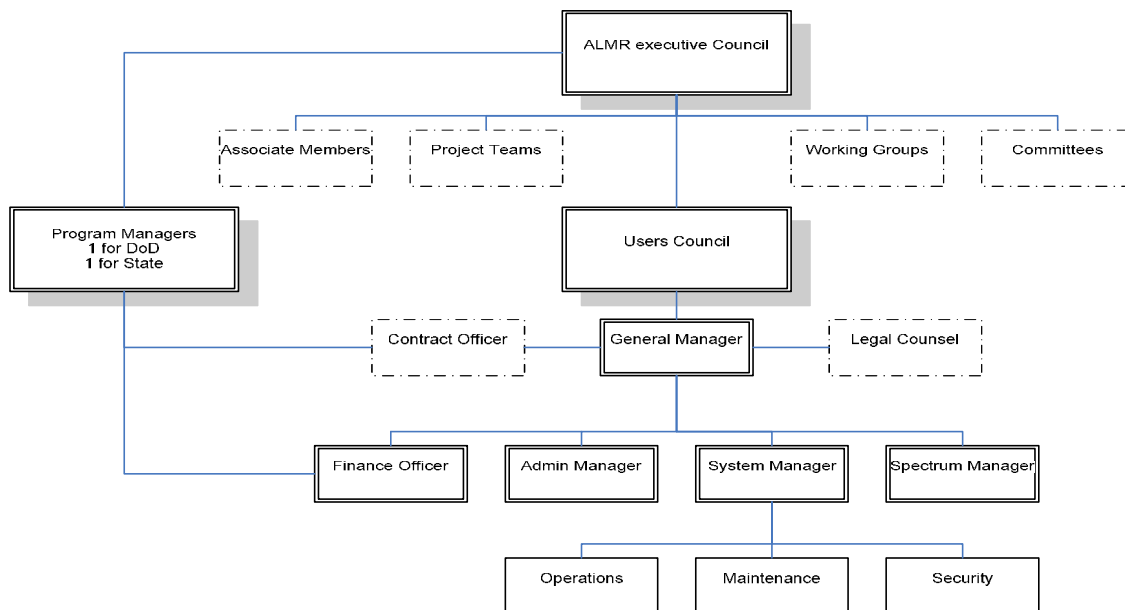
¹³¹ Alaska Land Mobile Radio Executive Council, *Charter For the Alaska-Wide Land Mobile Radio Executive Council*, Article 1 (Executive Council formed on September 19, 1995). The Charter for the ALMR’s Executive Council reflected intentions to work collaboratively across federal, state and local entities with the charge “to provide a common interoperable and cost effective LMR service that is compliant with federal, state and local regulatory guidance and is responsive to mission needs of all participating agencies in the State of Alaska.” *Id.*

¹³² *Id.* at Article III.

Furthermore, a noteworthy aspect of ALMR’s organizational structure is its strategic use of two program managers: one for DoD, and one for the State.¹³³ Especially during the Project build-out and in connection with securing funding for the system, this structure has produced significant benefits. In particular, it ensured that a person with agency-specific competence and insight could help ALMR navigate red tape-type hurdles and procedural idiosyncrasies of a given agency, thereby promoting administrative ease. For example, a DoD project manager could help secure access to a DoD facility in order for non-DoD personnel to construct an ALMR fixed infrastructure site.¹³⁴ Additionally, the dual program structure is advantageous with respect to steps associated with applications for Project funding such as protocols for such requests.

Significantly, the centralized leadership structure of ALMR is now effectively being diluted, a process that has been ongoing over the past two years. In general, ALMR’s morphing governance structure reflects a shifting project focus. Specifically, ALMR’s infrastructure build-out needs – while not entirely settled or complete – are now increasingly eclipsed by operational and system management challenges, including the need to be responsive to ALMR’s users and to recruit new local responders onto the network.¹³⁵ Accordingly, a more distributed and less centralized governance model has emerged to fit these needs. Figure 5 below illustrates the ALMR’s current organizational structure.¹³⁶

ALMR Operational Organization



¹³³ See Robert Howk, Alaska Journal of Commerce, *New Emergency Radio System Is Nation’s First* (October 20, 2003) (identifying State and DoD program managers); Robinson August 16, 2007 Interview, Note 82 *supra*.

¹³⁴ Smith August 16, 2007 Interview, Note 84 *supra*.

¹³⁵ See, e.g., ALMR, User Council Charter, Meeting Minutes, at 4 (January 4, 2006) (available at http://www.ak-prepared.com/almr/user_council.htm) (acknowledging user frustrations concerning “unknowns with ALMR,” including anxiety concerning local entities’ shares of operating costs for users going forward).

¹³⁶ See also SAFECOM *Grant Template*, Note 17 *supra*, at 19 (featuring similar organization chart reflecting ALMR as of March 2005). Additionally, ALMR’s stakeholders are currently contemplating a slightly different structure which would emphasize the role of the Municipal League in spearheading maintenance matters, the State of Alaska in leading on SATS-related issues, and the Executive Council and User’s Council concerning ALMR operations. Email message from Del Smith, dated August 21, 2007 (referencing Appendix B to draft Cooperative Agreement).

Figure 5: ALMR Organizational Chart

When viewed through the prism of Figure 4, these changes reflect a migration from a Lead Organization approach to a Network Administrative Organization. In at least two respects, ALMR's governance authority today is more distributed than in earlier years. *One*, although the Executive Council still retains formal power to approve ALMR activities, a User's Council was formed in 2006 which transitions ALMR to a mixed form of decision-making structure.¹³⁷ An increasing amount of responsibility is being pushed to the User's Council to identify system needs, service level requirements, and other operational aspects of the network, and on balance it is expected that the Executive Council will support most recommendations of the Users Council concerning these matters.¹³⁸ Once ALMR build-out and implementation is complete, plans call for the Users Council will assume leadership and "function independently" going forward.¹³⁹

Two, ALMR-specific managers (*viz.*, individuals employed by ALMR as an entity instead of by an ALMR member) such as an ALMR Operations Manager have been hired.¹⁴⁰ This development reflects an advisable strategy insofar as these hires reflect an insight concerning the separation of disparate management roles needed in a collaborative network: effective managers *of* a network are not the same as effective managers *within* a network.¹⁴¹ For example, an effective manager *of* a network's loyalties are to the network itself (*viz.*, the ALMR); an effective manager *within* a network's loyalties are primarily to his/her own employer organization (e.g., the DoD, the State Department of Administration, etc.). By hiring individuals whose primary loyalties are to the collaborative network itself (rather than split between the collaborative networks and a member of the network), ALMR's leadership better aligns the incentives of individual employees with the group's goals.

(iv) Political and Policy Risk: Negotiating the FCC/NTIA Handshake

Collaborative network efforts often trigger – sometimes intentionally, other times inadvertently – political and policy risks that must be addressed. This is not a trivial obstacle. For example, cross-agency collaboration in ALMR implicates Alaska's state statutes, state constitution, federal statutes, as well as numerous FCC and NTIA-related spectrum policy regulations.¹⁴² Just as many individual agencies are not generally architected for collaborative

¹³⁷ Membership in the Users Council is divided evenly among the four member organizations represented in the Executive Council. The twelve User Council member slots are divided as follows: three DoD representatives (one from the Army, one from Elmendorf AFB, and one from Eielson AFB); three federal non-DoD representatives (three votes, agencies yet undetermined at the time of writing for the Users Council Charter); three State of Alaska representatives (one from the Alaska Department of Transportation/Public Facilities, one from the Alaska Department of Public Safety, and one representing all other State of Alaska agencies); and three municipality representatives (one representing the Northern Region, one representing the Central Region, and one representing the Southern Region). Alaska Land Mobile Radio, *Users Council Charter*, Membership (January 11, 2006) (herein, "*Users Council Charter*," available at [www.ak-prepared.com/almr/pdf/ALMR%20Users%20Council%20Charter%20\(11%20Jan%202006\).pdf](http://www.ak-prepared.com/almr/pdf/ALMR%20Users%20Council%20Charter%20(11%20Jan%202006).pdf)). The Users Council's charge is to recommend "all operational and maintenance decisions affecting the ALMR Communications System." *Id.*

¹³⁸ *Id.*; Smith August 16, 2007 Interview, Note 84 *supra.*; Robinson August 16, 2007 Interview, Note 82 *supra.*

¹³⁹ This is subject to completion of the still-pending *Alaska Land Mobile Radio Communications System Cooperative Agreement*, which remains in draft form as of this writing. *Users Council Charter*, Note 136 *supra.* Authority. A Users Council attendee, Tech Sergeant Scott Blaine (a non-voting participant), describes the Users Council *esprit de corps* as follows: "The attendance from each agency during my time here [in Alaska] has been very good. There have been some definite advancements and many of the folks are enthusiastic and passionate about the work. Some of the document review work is hard to get volunteers but, overall, I'd have to say it's a good group." Telephone Interview of TSgt Scott A. Blaine, 3 CS/SCMEM (conducted August 6, 2007).

¹⁴⁰ For example, ALMR hired Del Smith as Operations Manager in March 2007 and, additionally, has contracted out systems needs to a third party manager. Smith August 16, 2007 Interview, Note 84 *supra.*

¹⁴¹ Milward and Provan, Note 63 *supra.*, at 57.

¹⁴² See AK ST § 29.35.010(13) (setting forth municipal governmental powers to enter into agreements); AK ST § 26.23.170 (directing DMVA to "evaluate the possibility of multi-purpose use of "a comprehensive state or state-federal telecommunications

network participation, the same can be true for the laws, policies and regulations which govern those agencies and their activities. Moreover, even when collaboration is permitted by existing laws, other practices can undermine cooperation. For example, ALMR's Project Manager noted that joint payments between different entities on a contract has occasionally proved problematic. For example, the State has at times had funds available to contribute the State's share toward payment on an ALMR contract between DoD and a third party contractor, yet the State's payment has been delayed by federal practices that would direct the money to the federal general treasury, not the specific contract at hand.¹⁴³

Changing political tides *within* a member entity participating in a collaborative network also generates risks for cooperative efforts. For example, while the State of Alaska is only one member of the Executive Council, the State itself is of course comprised of disparate agencies and actors. At any given time, these agencies and individuals can have countervailing priorities and needs; across time, leadership changes and agendas are altered. In ALMR, this phenomenon is reflected in the game of administrative ping-pong played with ALMR between the State's Department of Administration ("DOA") and the State's Department of Military and Veterans Affairs ("DMVA"). At the outset, ALMR was originally a DOA Project. DMVA had a stronger interest in its progress and success, however, since DMVA wanted ALMR for its emergency and public safety capabilities, while DOA was not anticipated to be a primary user of ALMR (and at that time had other projects underway).¹⁴⁴ In August 2004, following some inter-agency wrangling, ALMR responsibility was transferred from DOA to the DMVA. While this galvanized the State's involvement in the Project, the transfer had problems. For example, the State's 2005 appropriations associated with ALMR management went to DOA, not DMVA.¹⁴⁵ Moreover, although the 2004 transfer put ALMR primarily under the auspices of DMVA, the ALMR system still relied heavily on the State's SATS microwave network, controlled by the DOA. Not surprisingly, coordination between two rivalrous State administrative agencies was suboptimal.¹⁴⁶ Ultimately, the responsibility for the Project was transferred back to the DOA in 2007.¹⁴⁷ During the ALMR back and forth, the State's management of the ALMR program fell short in many areas, including recordkeeping, cost estimates, oversight, and local government outreach. Of course, all of these problems cannot be blamed solely on the contentious relationship between the competing agencies; however, DOA's early lack of enthusiasm and the resulting inter-jurisdictional rivalry generated political risks and costs which contributed to such problems.

Among political and policy risks faced by ALMR, however, the most impressive accomplishment has been navigating obstacles to spectrum sharing. In general, resource sharing invariably triggers the fear by users that "if I share now I will never get it back." In ALMR, participants wanted reassurance that, if they agreed to share at the outset, participants would retain their spectrum at the end of the sharing agreement. Accordingly, ALMR addressed this

network" for general state and local governmental purposes"); Article 10 Section 13 of the Alaska Constitution (concerning agreements and transfer of powers); 31 U.S.C.A. § 6305 (concerning when a cooperative agreement may be used as a legal instrument reflecting a relationship between the United States Government and a State or local government); FCC Waiver Order, *supra* Note 12.

¹⁴³ Callahan August 15, 2007 Interview, Note 79 *supra*. In such instances, DoD has had to re-enter a new contract which expressly references a cooperative agreement with the State, which has made it possible for payment by the State without losing control of the funds.

¹⁴⁴ Telephone Interview with Pat Davidson, Legislative Auditor, State of Alaska (conducted August 17, 2007); Callahan August 15, 2007 Interview, Note 79 *supra*.

¹⁴⁵ 2005 ALMR Audit Report, Note 86 *supra*, at 4.

¹⁴⁶ See generally DMVA Audit Response, Note 85 *supra*, at 1.

¹⁴⁷ State of Alaska FY2007 Governor's Operating Budget, *Department of Military and Veterans Affairs Alaska Statewide Emergency Communications Component Budget Summary*, p. 7 (December 2005) (available at http://www.gov.state.ak.us/omb/07_OMB/budget/DMVA/comp2781.pdf). The transfer was confirmed by CIO Michael Callahan. Callahan August 15, 2007 Interview, Note 79 *supra*.

fear through a Memorandum of Agreement between the DOD and the State of Alaska which provides that either entity “may revoke the authority to use” their spectrum in the ALMR project.¹⁴⁸

Most importantly, ALMR deserves considerable credit for its willingness to skillfully negotiate a regulatory thicket. ALMR representatives worked around provisions prohibiting the type of spectrum sharing which is a cornerstone of ALMR and arrived at a FCC/NTIA regulatory handshake which enables spectrum sharing. ALMR stakeholders had to obtain waivers from both the FCC and the NTIA in order to partner on the trunked radio system. To accomplish this, the State’s Interoperability Executive Committee was responsible for coordinating with the FCC and the Army Spectrum Management Office was responsible for coordinating waivers with the NTIA. Specifically, the waiver process for the FCC-controlled spectrum (*viz.*, 154.65 – 156.24 MHz) began in September 2002 when the State submitted three applications for waivers of Sections 2.102(c), 90.20(c)(3), and 90.173(c). However, before the process was over, Alaska learned that it would also require waivers to Sections 90.20(d) and 2.103(a).¹⁴⁹

Additionally, policy risks remained even after completing the required regulatory gauntlet and obtaining 92 waivers.¹⁵⁰ For example, waivers were conditioned upon build-out and loading requirements which – if unmet – potentially subjected the waivers to revocation. Short Alaska build-out seasons (especially in the northern part of the state) and the State’s administrative ping-pong with ALMR made this more than an idle concern and, ultimately, extensions to these requirements needed to be obtained.¹⁵¹ It should be noted that, while these results turned out to be unproblematic, political and policy risks could have proven a disaster had the spectrum waiver extensions been denied.

(v) **Technology Risk: Whither Project 25?**

A final risk factor stems from the tension between the desire to achieve interoperability by selecting a common standard. An agreed upon common standard facilitates interoperability. But due to the speed of advancing technology, as well as the mercurial nature of standards adoption in telecommunications, virtually any telecommunications venture runs the risk of becoming prematurely antiquated. ALMR selected the P25 standard for the operation of the network because it was the most mature interoperability standard available and also helped make the Project attractive for federal grant funds.¹⁵²

Nonetheless, despite the Department of Homeland Security’s (“DHS”) strong endorsement of the P25 standard, there remains significant technological risk associated with adopting and implementing it in a network. First, it remains to be seen whether or not the public safety community’s purchasing “tips” in favor of P25. A recent GAO report summarized some of the problems associated with P25 as a standard:

¹⁴⁸ Memorandum of Agreement Between Assistant Secretary of Defense for Networks and Information Integration and Commissioner Public Safety, State of Alaska, at 7 (July 25, 2003).

¹⁴⁹ FCC Waiver Order, *supra* Note 12, at 6. FCC discretion to grant waivers to rules is established in Section 1.925 of the Commission’s rules. There are two criteria for waivers: (1) granting of the waiver would be in the public interest; and (2) unique factual circumstances exist such that the rules become inequitable, unduly burdensome and contrary to the public interest, and no alternative exists.

¹⁵⁰ 2005 ALMR Audit Report, Note 86 *supra*, at 7.

¹⁵¹ Callahan August 15, 2007 Interview, Note 79 *supra*.

¹⁵² SAFECOM Grant Template, Note 17 *supra*, at 4 (section 2.02.4, providing that “equipment procurements involving new communications systems ‘should’ be compatible with the [Project 25] suite of standards”); GAO April 2007 Report, Note 20 *supra*, at 4.

P25 is “a suite of national standards that are intended to enable interoperability among the communications products of different vendors However, ambiguities in the published standards have led to incompatibilities among products made by different vendors, and no compliance testing has been conducted to ensure vendors’ products are interoperable.”¹⁵³

In addition to compliance testing shortcomings, P25 radios are expensive, costing between \$2,500 and \$5,500 each.¹⁵⁴ As noted in the GAO report, “Many localities do not have the funding to make such as large investment.” The high costs of P25 radios are often prohibitive for Alaska’s first responders, especially in rural and unincorporated areas where such responders must pay for their own radios.¹⁵⁵ Finally, the P25 standard does little to help public safety improve broadband capabilities.¹⁵⁶ P25 is a narrowband standard designed to provide voice communications for public safety agencies; it does not present a clear transition to broadband capability. Especially as public safety becomes increasingly aware of useful applications enabled by broadband capabilities, a rational course for some communities may be to spend less on narrowband radio systems and instead invest greater resources in broadband networks capable of providing a richer array of communications services. In short, if the public safety goals of providing interoperability and broadband capabilities merge into one network standard in the near future, then collaborative networks that have adopted P25 as a network standard will face difficult decisions about their transition to a broadband world.¹⁵⁷

C. Other People Problems – Such as Trust, Principal-Agent, and Collective Action Issues – Have Presented Significant Incentive-Related Challenges For ALMR

ALMR’s evolving governance structure, as described above, reduced organizational risk and enabled leadership tailored to dynamic challenges faced by the Project. Establishing an effective governance structure alone, however, is insufficient to create successful cross-jurisdictional collaboration. Significantly, collaborative networks demand that leaders and managers be attuned to the existing incentives of participants involved, ranging from the incentives of agencies participating in the network to the incentives of the individuals who work for those agencies.¹⁵⁸ People problems arising from incentive-related issues affecting a collaborative network can be categorized into three general areas: factors affecting trust,¹⁵⁹ principal-agent issues, and collective action problems. The following section examines each of these categories in turn below.

¹⁵³ *Id.*

¹⁵⁴ Alaska State Finance Committee minutes, April 12, 2006; *see also* GAO April 2007 Report, Note 20 *supra*, at 38 (noting that P25 radios are “prohibitively expensive” insofar as they are generally 2-3 times the cost of conventional radios).

¹⁵⁵ Callahan August 15, 2007 Interview, Note 79 *supra*. (emphasizing difficulty of receiving grant funds in unincorporated areas).

¹⁵⁶ Cramton *et. al.*, Note 34 *supra*, at 14.

¹⁵⁷ The highly configurable capabilities of software defined radios (SDR) may allow hybrid operations model. SDRs may be configured to operate for voice on the narrowband VHF band and operate for broadband applications in the 700 MHz band. Such applications of technology could provide significant benefit to users like the ALMR that have significant network infrastructure in place for the VHF narrowband network. Transitioning to a SDR would allow the agencies the ability to continue to receive benefits from their capital investments in narrowband network infrastructure while moving forward with broadband initiatives.

¹⁵⁸ In this vein, the National Governors Association (NGA) has highlighted the importance of providing incentives in order to achieve collaborative networks. For example, one strategy suggested by the NGA suggests that states “should consider a system that provides incentives to local agencies, as they are the most familiar with the needs of their first responders. For instance, if local agencies use the statewide infrastructure, they may not have to build their own infrastructure and the state may even purchase mobile radios for local police, fire, and EMS units.” *See* Governor’s Center *Strategies for Interoperability*, Note 41 *supra*, at 6. More generally, as James O’Toole has observed, leadership “is about understanding the differing and conflicting needs of followers . . . and energizing them to pursue a better end state.” James O’Toole, *Leading Change*, p. xi (1996) (Ballantine Books).

¹⁵⁹ One type of trust issue, *calculus-based trust*, is not addressed in this section. This is because research conducted to date has not collected significant information concerning the reputations of ALMR stakeholders prior to their collaborative efforts circa 1995.

(i) **Identity Based Trust Issues**

Identity-based trust flows from repeated direct interactions among participants in a network. Significantly, as a historical matter, Alaska enjoys a tradition of direct cooperation between agencies operating across vertical governmental layers. For example, extended cooperation between the State and the DOD helped develop Alaska's basic infrastructure including roads, bridges and communications.¹⁶⁰ Additionally, Alaska's geographic isolation from the lower 48 states also militates in favor of mutual assistance strategies.¹⁶¹ Overall, a baseline level of identity-based trust in Alaska existed prior to ALMR that made agencies amenable to working together on the Project. ALMR capitalized on the pre-existing relationships and has used two notable strategies – information flow and training exercises – to enhance the identity-based trust between participants.

First, the importance of information flow cannot be overstated in cultivating identity-based trust among members of a collaborative network.¹⁶² Information flow allows participating agencies to anticipate and diffuse issues related to differing cross-jurisdictional priorities as well as political or budget constraints that could adversely affect a collaborative network. In ALMR, the formation and structure of the Executive Council's four co-equal chairs helped ensure that the voices of major stakeholders would be part of the decision-making process. At its best, ALMR has also provided an admirable amount of transparency to stakeholders. For example, key documents, meeting minutes, and project progress are all easily accessible through the ALMR website.¹⁶³ Availability of this information keeps participants informed concerning the Project and attendant governance decisions. On the other hand, ALMR has not fully cultivated important relationship with many local responders, especially those in rural and remote areas. To help remedy this issue, ALMR in March 2007 hired an Operations Manager, Del Smith, a long time veteran of public safety whose responsibilities include improving information flow to local responders.¹⁶⁴

Second, joint training has further enhanced identity-based trust among first-responders by helping bridge boundaries between agencies more accustomed to operating within hierarchical silos. Indeed, one State official noted that training exercises which make interpretability “second nature” are critical since they develop the “people aspect” of interoperability, which is “a lot more difficult” than other dimensions of the ALMR Project.¹⁶⁵ Consistent with this emphasis, in December 2006 the ALMR leadership published a formal training plan for ALMR users.¹⁶⁶ This plan identifies the *who, what, when, where, how, and why* to perform training across the different agencies involved in the cooperative network.¹⁶⁷ The training plan raises awareness of potential benefits of ALMR's collaborative network and, moreover, promotes individual based trust by encouraging inter-agency training which strengthens the interpersonal relationships among individuals involved.

¹⁶⁰ John M. Brown III, *The Army in Alaska 2003: Installation Guide*, “A Message from the Commander,” 2003, at p.4-6, (available from <http://www.usarak.army.mil/2003%20Army%20in%20Alaska%20Guide.pdf>).

¹⁶¹ FCC Waiver Order, *supra* Note 12, at 2.

¹⁶² Telephone Interview with Pat Davidson, Legislative Auditor, State of Alaska (conducted August 17, 2007) (addressing the importance of free-flowing collaborative network communications which identify differing priorities and relative importance of initiatives among participating agencies).

¹⁶³ See Department of Military and Veterans Affairs, Alaska Land Mobile Radio web-site (available at <http://www.ak-prepared.com/almr/>).

¹⁶⁴ Smith August 16, 2007 Interview, Note 84 *supra*.

¹⁶⁵ Telephone Interview with Michael O'Hare, Department of Military and Veterans Affairs (conducted August 15, 2007).

¹⁶⁶ ALMR, *Alaska Land Mobile Radio Training Plan* (December 2006) (herein, “Training Plan,” available at http://www.ak-prepared.com/almr/pdf/010307%20Meeting%20Attachments/20061228_TrainingPlnV0_b.pdf).

¹⁶⁷ *Id.*

ALMR exercises from 2003 to the present have incorporated a wide range of responders – including DoD, non-DoD federal, state and local agencies – and trained them in the operational and technical use of the ALMR network. Most recently, the State, DoD and other federal agencies participated in a nationwide training exercise, *Ardent Sentry – Northern Edge '07*, which involved simulated attacks on infrastructure and military facilities throughout Alaska.¹⁶⁸ Such exercises familiarize ALMR users with Standard Operating Procedures (“SOP”) and the capabilities of a collaborative network.¹⁶⁹ A recent evaluation assessed the ALMR system as at an advanced stage of implementation with respect to training and day-to-day operations due to participants’ “familiarity and frequency of use.”¹⁷⁰

(ii) Institutional Based Trust

Institutional-based trust is developed through formal agreements and operational procedures among participants. Development of institutional-based trust responds, at least in part, to the presence of relationship risks (discussed in Part 3(B)(i) *supra*) where the division of responsibilities and lines of accountability are unclear between parties within a collaborative network. Additionally, promotion of institutional-based trust also reduces organizational risk (discussed in Part 3(B)(iii) *supra*) insofar as a collaborative network parties create formal structures to empower leadership and adopt management strategies. Accordingly, institutional-based trust is usually enhanced – and relationship and organizational risks are diminished – by the creation of effective formal safeguards. Ideally, agreements promote institutional-based trust by setting forth incentives which help align a participating agency’s interests with the collaborative network’s goals while constraining an entity’s ability to undermine the group’s collective efforts. Such agreements protect an entity against another participating agency’s shifting priorities and disparate goals.

While formal agreements appear to commit members to action, carve-outs may exist which effectively make such agreements aspirational rather than binding. For example, ALMR’s April 2001 Executive Council Charter provided that ALMR shall be operated subject to “the boundaries of federal, state, municipal *law* . . . [and the] *funding* and the *will* of each agency.”¹⁷¹ In function, this meant that a variety of factors – legal constraints, a lack of funding, or a waning of agency will (an amorphous concept, at best) – could each provide an independent excuse concerning failed contractual performance. Two reasons explain why ALMR’s Executive Council members have so far been comfortable with this: (i) the presence of other forms of trust; and (ii) as a practical matter (further discussed in Part 3(C)(iv) *infra*) the federal government has paid the majority of ALMR costs. As discussed in preceding sections, identity-based trust between collaborative network participants is well-developed among key ALMR stakeholders (especially the State and the DoD). Where the levels of other forms of trust – such as identity or calculus-based – are high, it might be expected that parties to a collaborative network will rely less upon the safeguards in formal agreements which promote institutional trust.

¹⁶⁸ United States Northern Command, USNORTHCOM News, NORAD- USNORTHCOM train in Ardent Sentry – Northern Edge '07, 12 May 2007, *By Petty Officer 1st Class Joaquin Juatai NORAD and USNORTHCOM Public Affairs available at* <http://www.northcom.mil/News/2007/051207.html>

¹⁶⁹ Tim Woodall, “Alaska Land Mobile Radio, Communications Planning and AS/NE '07 Readiness and Support,” 20 July 2006, p. 24 (available from http://www.nlectc.org/nlectcnw/download/woodall_asne_akinterop2006.pdf); Tim Woodall, *ALMR Program Overview: July 06 Interoperability Summit*, at 13 (PPT presentation listing four training exercises).

¹⁷⁰ Department of Homeland Security, *Tactical Interoperable Communications Scorecards: Summary Report and Findings*, at B-4 (January 2007).

¹⁷¹ *Memorandum of Understanding Between State of Alaska, Alaska Municipal League, Department of Defense Alaska Command, and Federal Executive Association of Alaska*, at 1 (MOU dated April 4, 2001) (emphasis added).

Significantly, a danger of underdeveloped formal agreements which are not well-enforced is that the project scope of a collaborative network is not sharply delimited. For example, ALMR experienced problems stemming from a State project manager's decision to approve four additional ALMR network sites without the consent of the Executive Council (as required by Charter).¹⁷² Afterwards, it was acknowledged that formal safeguards bereft of control of the Project's scope left ALMR vulnerable to such problems. The "project has never had a scope control philosophy or a documented process for making changes" and one person was able to act outside authorization.¹⁷³ The unapproved unilateral act led to the delay in the Project because funds were diverted to the unapproved sites and further progress had to wait for additional funding.¹⁷⁴

(iii) Principal-Agent Issues

Principal-agent problems arise where an agent's incentives diverge from a principal's objectives. In a public safety collaborative network, such difficulties are present when enhanced cross-jurisdictional interoperability would be in the best interest of the principal (*e.g.*, an ALMR member) but the incentives of individuals agents (*e.g.*, individual employees of a member) militate against cooperation. This is not extraordinary when entities consider whether to join a collaborative network involving different technology or systems. Under such circumstances, an individual agent responsible for an entity's existing network is faced with the loss of at least some autonomy over the system and, moreover, an agent may have (legitimate) concern that new system will entail personal change-over costs and not fit his or her existing competency.

In ALMR, principal-agent considerations have presented significant issues for system adoption by local responders. One principal-agent problem simply relates to costs. As discussed above, most local agencies need to upgrade their mobile radios to P25 compliant radios that cost between \$2300 and \$5500.¹⁷⁵ In rural and unincorporated areas, especially where costs must be borne by individual volunteers, this is a significant disincentive for individual users to want to join ALMR.¹⁷⁶ In addition, a second principal-agent problem stems from individual changeover costs associated with learning to install, operate and program new equipment once a new radio is purchased. Indeed, while reviews of the ALMR system's functionality have been positive, those involved with ALMR report that individual responder's resistance to learning how new radios and systems function can be an obstacle. For example, while the ALMR system expands the ability for responders to talk between one another, there is a learning curve involved in understanding talk group capabilities and other enhanced functionalities related to a trunked system since "you've got to think about who you're going to talk to."¹⁷⁷

ALMR evinces a best practice for overcoming principal-agent resistance – as well as to promoting identity-based trust – by providing ample training opportunities where individuals can acquire new skills needed to effectively function within the new collaborative network.¹⁷⁸ In ALMR, for example, the Executive Council has instituted National Incident Management System ("NIMS") training concerning cooperation between communications leaders in the new

¹⁷² See generally *DMVA Audit Response*, Note 85 *supra*, at 4.

¹⁷³ *Id.*

¹⁷⁴ Such activities exceeded not just the ALMR Charter, it also went outside the boundaries of Alaska law. The Project Manager was authorized to approve amounts up to roughly \$2,500, but blessing the four additional ALMR sites meant that the Project Manager authorized \$400,000. See *2005 ALMR Audit Report*, Note 86 *supra*, at 8-10.

¹⁷⁵ Alaska State Finance Committee minutes, April 12, 2006

¹⁷⁶ Callahan August 15, 2007 Interview, Note 79 *supra*. (in particular, indicating that federal grant programs have been problematic in reaching unincorporated areas where users might join ALMR if changeover costs were reduced).

¹⁷⁷ Smith August 16, 2007 Interview, Note 84 *supra*.

¹⁷⁸ DeSeve, *supra* Note 6, at 52.

network.¹⁷⁹ Further, the Executive Council has produced training materials to help communications leaders bridge the transition to the collaborative network.¹⁸⁰ More generally, in practice there is an additional inducement to overcome principal-agent resistance whereby ALMR provides its network infrastructure for free through a “beta” agreement.¹⁸¹ The beta program is a matter of necessity: until ALMR reaches “good use and condition” classification, user fees are not be collected because the network is still in the implementation phase.¹⁸² In function, however, it permits local agencies use of the network without paying user fees for the operation and maintenance of the network, which allows users – if they have radios – to use the network and experience the capabilities of the benefits of a collaborative network without making a long-term financial commitment.

(iv) **Overcoming Collective Action Problems**

Collective action problems – similar to principal-agent issues – involve incentives which can derail development and operation of a collaborative network. Collective action issues are present when an individual agency’s rational course is inconsistent with actions needed to help achieve the good of the collaborative network. Especially when participating in large collaborative networks, incentive exists for an individual agency participant to provide less than its share of resources to the group effort and, instead, attempt to free ride on the efforts of others.¹⁸³

For ALMR, in addition to the principal-agent issues detailed above, attempts to get local users to join the system have also met collective action-type obstacles. In part, this stems from the way that users internalize public safety costs. Current policies provide little incentive for public safety agencies to internalize the costs of spectrum usage. In particular, public safety responders do not face the opportunity cost of their spectrum and, accordingly, do not fully value the “free” spectrum pooled by State and federal resources in the ALMR system.¹⁸⁴ This is because NTIA and FCC public safety spectrum license assignment procedures effectively provide spectrum to agencies for free and, moreover, prohibit sale or lease of such licenses.¹⁸⁵

In contrast to spectrum costs, however, public safety agencies internalize the costs associated with the purchase of radios, as well as the build-out and operation of their networks. In particular, local entities – especially small entities that have not changed their LMR systems for decades and are unaccustomed to significant public safety communications expenditures – are highly sensitive to costs imposed by user fees and radio equipment costs. Although local responders realize some benefits from shared infrastructure (for example, increased capabilities to coordinate with other responders within their jurisdiction and improved communications during an emergency incident), their day-to-day benefits are likely to be significantly lower than for State and DoD responders, who regularly travel across jurisdictional boundaries and benefit from the extended footprint enabled by extended network coverage. Accordingly, State and federal

¹⁷⁹ Timothy Woodall, Alaska Land Mobile Radio, “*Communications Planning and AS/NE '07 Readiness and Support*,” at slide 11, (20 July 2006) (available from http://www.nlectc.org/nlectcnw/download/woodall_asne_akinterop2006.pdf).

¹⁸⁰ See, e.g., Training Plan, Note 166 *supra*. Also, the Executive Council has prepared an “ALMR Preparedness Checklist” for communications leaders which identifies the key areas that require action in order to successfully become part of the ALMR network. ALMR, “*ALMR Preparedness Checklist*,” (available from <http://www.ak-prepared.com/almr/pdf/Preparedness%20Checklist.pdf>).

¹⁸¹ There are two network sites that preparation and equipment purchase is the responsibility of the municipal government. They are the City and Borough of Juneau and the City of Valdez.

¹⁸² Robinson August 16, 2007 Interview, Note 82 *supra*.

¹⁸³ Brito, Note 48 *supra*, at 464.

¹⁸⁴ Callahan August 15, 2007 Interview, Note 79 *supra*. (local agencies “could not care less” about the spectrum issues; local responders’ primary concern is that then they “push to talk, that it works”).

¹⁸⁵ See Brito, Note 48 *supra*, at 474 (explaining that public safety agencies “do not face the opportunity cost of the spectrum they are given by the FCC”); Cramton *et. al.*, Note 34 *supra*, at 33 (spectrum “free” from public safety perspective).

entities should be expected to weight the benefits of the collaborative network more heavily, and local responders can be expected to be less committed to the system and more inclined to ride on others' efforts and resources.¹⁸⁶

To date, this has been the case in Alaska. Indeed, collective action problems – especially concerning local agency involvement – have been surmounted mostly by the emergence of a project “champion” willing to pay a disproportionate share of the network build-out.¹⁸⁷ The DoD has championed the Project from its inception and, more recently, the State of Alaska has emerged as a second champion. As noted above, federal responders were originally motivated to join ALMR because of requirements relating to the NTIA’s narrow banding specifications.¹⁸⁸ Significantly, following the terrorist attack of September 11, 2001, the DoD identified gaps in the nation’s homeland defense capabilities. In order to fill those gaps, the U.S. Northern Command (“NORTHCOM”) was created to deter, prevent, and defeat threats and aggression aimed at the United States. Within Alaska, the Joint Task Force (“JTF”) Alaska was created to enhance military readiness in the region, protect infrastructure, and to coordinate assistance to civil authorities. This new mission and responsibility motivated the DoD to ensure the ALMR network was completed, at least to a level that would allow them to accomplish this mission.

The role of the DoD as a champion is evident in several aspects of the Project. Overall, the federal financial commitment has been critical to ALMR: a recent estimate put federal funding at 85% of an estimated \$120 million Project price tag.¹⁸⁹ Consistent with this commitment, when the State failed to allocate sufficient funds to do site preparation work in 2005, the DoD helped the State complete preparations on 11 sites.¹⁹⁰ Indeed, at one point in 2005, it was estimated that the DoD’s contribution to the Project was \$55 million compared to the State’s investment of \$3.5 million.¹⁹¹ Moreover, when the State struggled with managing the implementation of the network, DoD remained a supportive and committed partner to the Project in order keep the collaborative project together.¹⁹² Finally, in addition to financial support, Tim Woodall has served as the DoD’s Program Manager, where he has played a catalyzing role at virtually all stages of the Project.¹⁹³

A salutary effect of a project champion is that a project’s legitimacy is enhanced.¹⁹⁴ Moreover, especially for government projects, initial buy-in can be the most important step because “when a project has been approved through the political process and is deemed crucial to the public interest, government will very seldom abandon it. Public organizations will usually

¹⁸⁶ The important exception to this, of course, is where federal dollars are available to local entities for adoption of interoperable public safety systems. But discussions with first responders in Alaska – as well as elsewhere – confirm that absent a large portion paid for by grants, rural responders are highly sensitive to user fees and costs of new radios. See, e.g., Callahan August 15, 2007 Interview, Note 79 *supra*.

¹⁸⁷ It has been noted that public safety projects sometimes benefit from the emergence of a champion or outspoken leader who has the political clout to get things accomplished. U.S. Department of Justice and U.S. Department of Homeland Security SAFECOM Program, *2006 National Interoperability Summit Proceedings*, Prepared by SEARCH The National Consortium for Justice Information and Statistics, at 20 (May 24-25, 2006) (herein, “2006 National Interoperability Summit”) (available at <http://www.search.org/files/pdf/2006InteropSummitProceedings.pdf>).

¹⁸⁸ Deputy Secretary of Defense, *Memorandum for Secretaries of the Military Departments Service Acquisitions Executives, Assistant Secretary of Defense, Special Operations and Low-Intensity Conflict, Directors of the Defense Agencies, Director, Joint Staff: Policy for Land Mobile Radio (LMR) Systems* (August 1, 2001).

¹⁸⁹ Carolyn Marsan, NetworkWorld.com, *Alaska’s Wireless Net Built for Emergency* (August 28, 2006). As of March 2005, the DoD had itself provided over \$55 million in funding. MG Campbell Testimony March 23, 2005, Note 100 *supra*, at 7. Estimated total costs to complete the system have fluctuated over the years and appear to be between \$120-150 million. See *2005 ALMR Audit Report*, Note 86 *supra*, at 8-10 (discussing fluctuating estimated costs).

¹⁹⁰ *2005 ALMR Audit Report*, Note 86 *supra*, at 9, 19 (delays shifted “a large part of the work, and associated cost, to DoD”).

¹⁹¹ MG Campbell Testimony March 23, 2005, Note 100 *supra*, at 6-7.

¹⁹² *Id.* (reassuring Senate Committee that DoD would not withdraw from ALMR despite rumors of “uncomfortable” working relationship with the State).

¹⁹³ See generally Robinson August 16, 2007 Interview, Note 82 *supra*.

¹⁹⁴ Milward and Provan, Note 63 *supra*, at 58.

restructure a project if they encounter significant problems, and will keep adding more resources until the Project is completed.”¹⁹⁵ In any event, it is clear that the DoD’s commitment to ALMR increased belief that the Project would come to fruition, which in turn promoted buy-in by the State. Significantly, over the past two years, the State has assumed a champion-like role by providing substantial support from its general funds.¹⁹⁶ Additionally, since March 2007, the State has initiated a more concerted effort to recruit local and State agencies to become users of the ALMR network.¹⁹⁷

PART IV. CONCLUSIONS AND NEXT STEPS

This paper frames public safety interoperability hurdles as part of the larger challenge concerning cross-jurisdictional collaborative networks. This perspective helps identify the elemental tension present when agencies, which are generally built to resolve problems within their jurisdictional boundaries, attempt to capture 21st Century network effects by working across jurisdictional boundaries. Issues that flow from this tension – so-called “people-problems” – can be understood through the prism of a coherent framework which teases out the risks and incentive-related problems of collaborative networks. To date, most interoperability discussions focus more narrowly on public safety-specific problems and best practices. As efforts continue to promote improved interoperability, however, a broader analytic framework should help collaborative network participants anticipate and trouble-shoot issues which, if undetected, might undermine or retard the initiative. This paper attempts to provide such a framework built around risk factors, dimensions of trust, as well as principal-agent and collective action issues. This is an early effort toward development of a coherent framework and further work would be worthwhile.

Especially when viewed through an analytic framework, ALMR’s 12 year history presents a rich case study of a collaborative network designed to improve public safety interoperability. ALMR’s operational results include shared use of network infrastructure, extensive federal involvement, spectrum pooling, improved operational coordination, and expanded public safety network coverage. While ALMR’s operational achievements are notable, the Project’s experience concerning risks and incentive-related problems are especially telling. This paper’s analysis illustrates certain prescient and advisable ALMR strategies, including skillful reduction of political and policy risk by obtaining spectrum sharing waivers from the NTIA and FCC, utilization of a dual project manager structure to reduce organizational risk and promote administrative efficiency, the emergence of a champion to overcome collective action problems, and extensive use of training to enhance identity-based trust. It also illustrates ill-advised or uncertain courses of action, including the failure to anticipate or adequately manage political risk associated with rivalrous State agencies concerning the Project, shortcomings in addressing relationship risks between ALMR and local users, and technological risk associated with promoting a standard which invites principal-agent problems associated with expensive products.

Collectively, the analytic framework and the ALMR case study underscore a simple

¹⁹⁵ Préfontaine, Note 58 *supra*, at 7 (Centre Francophone D’Informatisation des Organizations 2003) (part of *New Models of Collaboration* study spearheaded by Center for Technology in Government at University at Albany, SUNY, materials available at http://www.ctg.albany.edu/publications/online/new_models/essays/risk).

¹⁹⁶ 2005 ALMR Audit Report, Note 86 *supra*, at 9.

¹⁹⁷ Smith August 16, 2007 Interview, Note 84 *supra*. While local user buy-in remains in question, the legitimacy engendered by State and DoD commitment has induced at least some additional users to join who might have otherwise waited to see if the effort succeeded before joining.

insight and corollary. The insight: it is hard to establish successful and sustainable collaborative networks. The corollary: achieving public safety interoperability is hard. To be clear, this is not to suggest that interoperability initiatives should be curtailed. Indeed, public safety agencies cannot and should not ignore the opportunity to leverage capabilities made possible by the enhanced power of networks. Rather, the upshot of this paper's insight and corollary are three-fold.

First, our analysis cautions that interoperability challenges should not be underestimated. "People problems" are formidable obstacles that require careful planning, savvy strategy, and – more than likely – significant funding. Rather than seeking perfection, interoperability planning should be oriented around solutions likely to minimize people problems en route to substantially improving the *status quo*. Further, while ALMR's organizers have evinced admirable vision, analysis shows that ALMR is not an easily replicable model for other states and regions to emulate. Indeed, ALMR's interoperability efforts are in several important respects *sui generis*: ALMR has benefited from a pre-existing baseline of strong identity-based trust; the DoD emerged as a deep-pocketed champion to help surmount collective action issues; and Alaska's policy-related risks concerning spectrum sharing were somewhat mitigated by relatively low spectral congestion which is a function of Alaska's low population density.

Second, while technology exists today to enable interoperable communications, additional solutions are needed to help bridge people problems and improve network coordination and efficacy. In particular, it should be considered whether three smart radio capabilities could help reduce risk and incentive-related issues in the public safety context: (i) *cognitive capabilities*, including a *policy engine* which could facilitate trust and reliability across entities by putting agreed upon procedures (such as SOPs), understandings (such as Memorandums of Agreement and Mutual Aid Agreements), and protocols (such as ICS) into machine readable language to govern operation of devices on the network; (ii) *software defined capabilities*, including an ability to alter talk groups and use frequency agility to help perform bridging functions in a manner which reduces spectral congestion; and (iii) *ad hoc networking capabilities*, which could expand coverage of existing public safety networks. Further work on these ideas is warranted.

And *third*, perhaps the most important upshot of this analysis is that people problems are not going to go away. It is true that the transition for public safety agencies to next generation interoperable networks – in particular, the transition from a silo-network perspective to a collaborative network-of-networks mentality – will be particularly difficult for public safety responders. Nonetheless, even after cross-jurisdictional next generation networks are established, the problems of collaborative networks will remain absent the unlikely radically re-design of public safety agencies. That is, so long as agencies built to resolve problems primarily within their boundaries are required to work collaboratively, fundamental risks and incentive-related problems will persist.

APPENDIX A
Sample Definitions of Interoperability

Entity	Definition	Source
United States Congress	“the ability of emergency response providers and relevant Federal, State, and local government agencies to communicate with each other as necessary, through a dedicated public safety network utilizing information technology systems and radio communications systems, and to exchange voice, data, or video with one another on demand, in real time, as necessary.”	PL 108-458, The Intelligence Reform and Terrorism Prevention Act of 2004 ¹⁹⁸
Federal Communications Commission	“an essential communications link within public safety and public service wireless communications systems which permit units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results”	47 C.F.R. § 90.7
National Association of State CIO (NASCIO)	“Interoperability has different meanings depending on the context, however, in the public safety arena the term is generally understood to mean the ability for public safety agencies and public services to talk to one another via radio communications systems and/or share information with one another accurately, on demand, in real time, when needed, and when authorized.”	NASCIO Research Brief, <i>We Need to Talk: Governance Models to Advance Communications Interoperability</i> (November 2005) (quoting NASCIO’s Interoperability and Integration Committee) (available at http://www.nascio.org/publications/documents/NASCIO-InteropGovResearchBrief.pdf)
Department of Homeland Security’s (DHS) Project SAFECOM	“The ability of public safety agencies to talk across disciplines and jurisdictions using radio communication systems, exchanging either voice or data with one another on demand, in real time, when needed, and as authorized.”	<i>SAFECOM Grant Template: Roadmap to Beneficial Use Critical Plans</i> (March 31, 2005)
General Accounting Office	“Interoperability in the context of public safety communications systems refers to the ability of first responders to communicate with whomever they need to (including personnel from a variety of agencies and jurisdictions), when they need to, and when they are authorized to do so. It is important to note that the goal of being able to communicate when necessary and authorized is not the same as being able to communicate with any other individual at any time—a capability that could overwhelm the communications infrastructure and would likely impede effective communication and response time.”	United States Government Accountability Office, <i>FIRST RESPONDERS: Much Work Remains to Improve Communications Interoperability</i> (April 2007)
International Association of Fire Chiefs	“Operational interoperability is the ability to work together effectively. Specifically, it is the ability of different jurisdictions or disciplines to provide services to and accept services from other jurisdictions or disciplines, and to use those services to operate more effectively together at an emergency . . . Technical interoperability is the ability to communicate and exchange information. More formally, it can be defined as the ability of systems to provide dynamic interactive information and data exchange among command, control and communications elements for planning, coordinating, integrating and executing response operations.”	William L. Pessemier, TOP PRIORITY: A Fire Service Guide to Interoperable Communications at 3 (The International Association of Fire Chiefs, 2006) (herein, “Fire Service Top Priority”) (available at http://www.interoperability.virginia.gov/pdfs/FireService-InteropHandbook.pdf).

¹⁹⁸ Cited in *Aspen 2006 Emergency Communications*, Note 26 *supra*, at 3-4.

