Smart Radios and Collaborative Public Safety Communications

Brad Bernthal* and Nancy Jesuale** [++]

Smart radios should play a pivotal role in addressing difficult organizational behavior issues which frustrate the migration of public safety communications toward extensive inter-organizational collaboration. This paper frames how non-technical hazards – such as mutual distrust, cultural frictions, inexperience in cooperative settings, and policy obstacles – present significant challenges to public safety cooperation. We further explain the collaborative advantage to be gained by migration toward a cooperative, federated network architecture. Finally, we emphasize how smart radio technologies could facilitate trust building and control mechanisms in inter-organizational relationships. Over time this will increase confidence in cooperation. Accordingly, we advance a perspective which bolsters the case for extending advanced military smart radio research into the development of public safety and homeland security advanced communications architectures.

* Brad Bernthal, Associate Clinical Professor, University of Colorado Law School, Boulder, Colorado. (303.492.0610, brad.bernthal@colorado.edu).
**Nancy Jesuale, President and CEO, Net City Engineering.
[++] The authors thank Ryan Day for excellent research and assistance drafting portions of Section III(C), and Nandini Kembyranna Shankarappa for her efficient citation and format work. The authors are grateful for comments and suggestions on prior drafts from Phil Weiser, John Chapin, Dale Hatfield, Nick Alexander, Curt Knight, and Mark Pallans.

Table of Contents

I. INTRODUCTION

Satisfying first responders' communication requirements through trust building and collaboration – as opposed to relying on physical network segregation to mitigate risk – is the most critical challenge faced by advanced public safety network architects. In particular, public safety communications' capabilities must be enhanced through cooperation and sharing without unduly compromising local agency control over essential aspects of their networks. Diversity among the thousands of first responder organizations in the United States, ranging from large urban police departments to rural volunteer fire departments, as well as cultural aspects of the local governments who operate them, dictates that a strong local control requirement must remain a feature of public safety radio systems. Consequently, there exists a critical need for innovation that can meet the *capability* requirements for public safety advanced networks while still accommodating a first responder agency's *trust* requirements.

Much attention has been paid over the past decade to the need for public safety responders (*e.g.*, fire, police and emergency services) to be able to communicate across organizations. Yet a viable strategy to enable inter-organizational collaboration must chart a tricky path. There remains insistence that public safety agencies should own their own land mobile radio ("LMR") systems while using dedicated public safety frequencies. [1] Exclusive ownership equates to control. Traditionally, this exclusive form of control is the only one trusted when first responders' lives are on the line. This has resulted in disparate communications systems operating across different frequencies on a city-by-city and even agency-by-agency basis.

[1] Traditional LMR systems are often tailored to the communications needs of individual first responder agencies, such as a jurisdiction's fire, police or emergency services. Most systems today remain optimized for voice traffic. In contrast to traditional LMR systems, the 700 MHz "D-Block" provided hope of catalyzing greater uniformity in public safety broadband data communications. The future direction of the D-Block is unclear, however, following the 2008 auction which failed to reach the prescribed reserve price [47]. Meanwhile, unlike the D-Block approach which targeted the same block of 700 MHz spectrum, existing public safety LMR frequencies are scattered across the spectrum. Federal authorizations are between 136-174 MHz, 360-400 MHz, and 402-420 MHz, while local agency assignments are between 136-174 MHz, 450-512 MHz. Public safety users are also in the 700 and 800 MHz bands [1]. The 700/800 MHz bands are most popular for urban users while the lower UHF and VHF bands are better suited to rural users [2]. An additional 50 MHz has been allocated by the FCC to public safety in the 4.9 GHz band. Each agency is assigned licenses to use their own dedicated radio frequencies. Formally, state and local first responders receive "licenses" assigned by the Federal Communications Commission. Meanwhile, federal responders – ranging from the FBI to the Department of Defense – receive "authorization" from the NTIA. While the nomenclature difference is not significant for this paper, the dual management structure of spectrum does represent an additional coordination challenge for public safety communications collaborations.

Obvious solutions to this problem are elusive. For example, a unified, nation-wide LMR technology switch is unlikely to occur in view of current scattershot of frequency assignments, a dual spectrum management regime between the FCC and NTIA, and funding cycles which are painfully slow and inadequate [1]-[3].

Nonetheless, policy-makers must somehow catalyze sweeping change in the structure of public safety communications. Problems engendered by today's exclusive and balkanized systems include shortcomings in advanced capabilities (such as user and application prioritization, sharing and roaming, and authentication of users) as well as inadequacies in other dimensions of public safety radio performance (such as interoperability and spectrum access). While near-term policy objectives must succeed within the realities of current constraints, foresighted public safety policy should not reinforce today's imperfections by locking in a silo-oriented architecture going forward. Significantly, we propose that smart radios can assist migration to a next generation communications architecture by providing a technological means to gracefully advance public safety toward a collaborative paradigm.

This paper attempts to make three contributions. *First*, we identify the need to align the vision for advanced collaborative public safety networks with the goals and incentives provided to state and local public safety stakeholders. Current federal research is redefining public safety's communications requirements so as to include enhanced mobility and coverage (even where infrastructure is unavailable), an ability to communicate across a range of frequencies, flexible and dynamic system administration, and policy-based radio capabilities based on machine-readable policies which determine whether the radio may operate.[2] Yet there remains a chasm between the advanced networking research community's vision for evolved communications and the support and information currently provided to public safety stakeholders "on-the-ground" necessary to implement such a vision. We recommend that this gap should be bridged.

Second, we explain that public safety inter-organizational cooperation is foremost not a technical problem but, rather, a difficult challenge involving policy incentives, governance, legal contracting, and organizational behavior. No matter how good the technology, a failure to resolve non-technical issues will result in wasted money and failed systems. Notably, a common thread underlies most visions of advanced public safety communications: *extensive collaboration* between organizations. That is, in order to realize the promise of next generation communications, success hinges on sharing and cooperation sufficient to permit a federated (*viz.*, shared, but not owned) public safety communications architecture. A critical

[2] Machine readable policies could incorporate existing regulatory policies as well as other transmission constraints provided to the radio.

aspect of today's public safety communications struggles, however, concerns the tenacity of non-technical barriers to cooperative relationships. Current public safety "interoperability" shortcomings represent only one manifestation of a wider set of limited capabilities caused by a fragmented approach to systems deployment and spectrum management. In this paper, we view public safety communications "problems" primarily through the lens of organizational behavior by emphasizing the role of trust and risk in collaboration.

And *third*, we explain why smart radio devices should play an important role in facilitating and implementing collaborative strategies. By smart radios, we mean software defined radios ("SDR") and policy-based cognitive radios ("CR"). [3] We propose that the catalyst for smart radio in public safety will be policy-based software controls and administration. Policy-based software will enable local control, however, such controls will be provided at higher network layers, rather than the traditional separation of public safety networks at the physical layer. Importantly, *policies are the architecture* for smart radio networks insofar as machine-readable policies provide the defining attributes concerning how radios operate (or not) given the broader constraints of a system's infrastructure.

It should be noted that a rush to expansive collaboration between entities often results in failure. Cooperation will take time and should be facilitated through focused and graduated collaborative successes. Significantly, as public safety stakeholders work together to define trusted policies, smart radios should play a pivotal role in the trust-building process between entities in a way that today's traditional LMR technologies cannot. For example, the types of sharing an entity agrees to within a smart radio architecture remains a matter of local control, yet such policies can be dynamically altered and reconfigured over time. This enhances both the chances of successful collaboration as well as increasing the willingness of agencies to collaborate. As entities build trust and collaborative competency, they will then be able to migrate toward an advanced public safety radio architecture.

Following this Introduction, Section II next analyzes recent research which underscores potential collaborative advantages available to public safety. Achieving this vision, however, requires migration away from segregated public safety systems, which evolved as a result of deliberate architectural choices. Section III then explains how organizational challenges must be squarely addressed in order to achieve successful inter-organizational collaboration. The role of trust and risk is emphasized and we suggest that trust-building loops and control mechanisms should be used to promote confidence in collaboration. Finally, in Section IV we propose

[3] Software defined radio (SDR) and policy-based cognitive radio (CR) are more fully discussed in Section IV(A) *infra.*

how smart radios can assist in this process. In particular, reconfigurable software policies could enable both local control and graduated levels of cooperation. Each of these is addressed in turn below.

II. TOWARD AN EXPANSIVE VIEW OF PUBLIC SAFETY COLLABORATION

Shortcomings in public safety networks arise from today's network architectures which are segregated from one another by technological design. As explained in Part A, these technical firewalls exist by choice, not by accident. Part B next identifies recent research and reports which underscore that expanded collaboration will be required to meet the needs of first responders. Accordingly, this Section II makes clear that an architectural shift is required as next generation network developers consider how public safety systems can be oriented around collaboration instead of separation.

A. The Need for Public Safety Collaboration

Public safety in the United States today is "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."[5] Interoperability is the "ability of emergency responders to communicate among jurisdictions, disciplines, and levels of government, using a variety of frequency bands, as needed and as authorized." [6],[7][4] Although interoperability improvements in local and state first responder radio systems have been the focus of much effort and investment on the part of federal, state and local government in the U.S.,[5] it is becoming clear that interoperability issues cannot be solved by solutions which band-aid two or

[4] Bernthal *et. al.* in [7] identified a "family" of six interoperability characteristics based on an examination of academic commentary, reports, and legislation. These six traits include: the ability of emergency response providers (and, often, other public service providers) to communicate between vertical governmental levels (*viz.,* federal-state-local); (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); (iii) the ability to perform under a common command-and-control structure to achieve predictable results; (iv) access to networks that enable robust and real-time communications between responders, including voice, data, and video capabilities; and (v) the capability to rapidly authorize users without compromising secure communications. While not often expressed in formal definitions of interoperability, discussions almost uniformly include a sixth characteristic: the ability to rely on accepted standards which promote and certify interoperable communications capability

[5] An estimated $4.9 billion in federal grants for interoperability was provided over five years from 2003-08 [4].

more existing LMR systems together. Department of Homeland Security Secretary Michael Chertoff has emphasized that "technology by itself is not a magic bullet" and "the biggest barrier to interoperability is not technology . . . It has to do with, rather, human beings."[8]-[10] Secretary Chertoff recently put a fine point on the problem of non-technical hazards faced by collaborative networks[8]:

> If you do not get [ ] agreement among the responders in the field, no amount of technology is going to allow them to communicate with each other . . . Technology only works in the context of a system, which has been designed to achieve an end. A system [must consider] human factors and the incentive structure, or the microeconomics of how we live as well as the gizmos and gadgets which you all are out there investing. It is only as part of a whole system that these gizmos and gadgets actually make sense.

Today's lack of interoperability, deficiencies in enhanced capabilities like roaming, and coverage problems between multiple public safety LMR systems are not fundamental implementation failures, but rather the consequences of *successful* implementation of designed architectural separation. Broadly speaking, most public agencies are chartered to address problems within their own jurisdictional purvey, not for extensive inter-organizational collaboration[11].[6] Not surprisingly, public safety communication systems mirror this approach and evolved in "siloed" systems. An over-arching notion of public safety "exceptionalism" – *viz*., an individual public safety organization's communications needs are simply too unique, too specific to an individual agency's demands, and too hierarchical for inter-organizational collaboration – reinforced this approach. Consequently, public safety spectrum policy and technologies traditionally worked together to create wireless system deployments that are by design private to a single or specific user group, limited in geography to a jurisdiction's boundaries, operational only in limited radio bands, and secured at the physical layer by keeping non-owners off of the system. In short, the prevailing approach mitigates risk through separation.

In view of today's technological enablers, however, current problems facing first responders present an opportunity for fundamental reevaluation of architecture oriented around collaboration. Next generation first responder networks will need to be designed so as to meet an agency's

[6] As noted in [11], "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."

expanded needs (for example, broadband applications and roaming), be available to surrounding agencies to enable interoperability and perhaps reduce costs, and be designed so as to be compatible with surrounding networks. Over the long term, we envision three dimensions of infrastructure and spectrum sharing involving public safety: (i) vertically between federal, state and local communities; (ii) horizontally across jurisdictional boundaries; and (iii) inter-sector relationships which enable roaming between public safety and commercial and business/industrial licensees.

B. Research and Development Recognizes Collaborative Benefits

A growing number of recent federal research reports signal the value of more collaborative approaches to public safety architectures. In this subsection, we analyze several reports which collectively underscore a paradigm shift concerning wireless public safety communications requirements. Specifically, we distill the following needs suggested by recent federal and industry research and development efforts [12]-[23]:

- Enhanced mobility and coverage, even where infrastructure is unavailable;
- Shared network requirements incorporating secure authentication, prioritization of users, and mechanisms for interference protection;
- Ability to establish *ad hoc* networks;
- Frequency agility and frequency sharing;
- Multi-band operation;
- Flexible and dynamic system administration; and
- Policy Based radios.

Support for the public safety requirements reflected in the above bullets is supplied by recent research and reports. The balance of this subsection expands upon these reports.

The *Federal Plan for Advanced Networking Research and Development* provides a notable roadmap for technology research and development in order to meet advanced networking requirements [12],[13]. In 2007, the National Science and Technology Council (NSTC) Committee on Technology established the Interagency Task Force on Advanced Networking (ITFAN) to address myriad problems related to federal networking needs. Significantly, the ITFAN recognized the importance of networking innovation for emergency response because “today’s networks have become captive to the limitations and vulnerabilities of the current

generation of technologies."[12][7] To achieve necessary advanced networking capabilities, the ITFAN focused on four major goals:

1. Provide network services anytime, anywhere;
2. Make secure global federated networks possible;
3. Manage network complexity and heterogeneity; and
4. Foster innovation through development of advanced network systems and technologies.

A major contribution of the ITFAN roadmap is the concept of federation among heterogeneous networks. Specifically, the report provides that [12]:

> The increased complexity of future networks requires thinking outside of traditional models for network research (i.e. focused on specific technologies) to the *development of architectures and frameworks that can integrate many technologies* to deliver the services needed for mission accomplishment. (Emphasis added.)

A second major contribution of the ITFAN roadmap is the recognition that wireless networks will evolve toward policy-based *ad hoc* networking relying on dynamic spectrum access ("DSA"). The third major contribution is the recognition that federated networks will serve multiple classes of users (*e.g.,* government, industry and academia) and that architectures will no longer be single user or single purpose (*e.g.,* health care vs. transportation).[8] Heterogeneity in architectures could mean the federation of wired and wireless infrastructures, using multiple frequency bands, different topologies, and different access policies.

A report from the National Research Council of the National Academies, *Improving Disaster Management, The Role of IT in Mitigation,*

---

[7] More generally, [12] recognized that:

> the Federal government depends upon ***fundamental advances in networking technology*** for enhancing a wide range of applications including emergency response, national security and emergency preparedness communications, defense mission support, health care information technology, secure economic transactions, distributed intelligence applications, and advanced scientific computing. These applications share a need for ***faster, more secure, more reliable and more robust networks*** than are currently available.

[8] As indicated by the inclusion of industry and academia, next generation networks will not be single purpose public safety only networks, but will carry a variety of traffic, applications, etc. over a federated infrastructure. Users will be segregated by policies and security protocols.

Preparedness, Response, and Recovery, also underscored the need for more advanced capabilities [22]. In the wake of Hurricane Katrina and the 9-11-01 domestic terrorism attacks, the Administration and Congress took measures to identify the reasons why communications systems used by federal, state and local disaster response entities fail to provide adequate communications for first responders on the scene, and why technologies to support situational awareness for emergency managers are lacking. The National Academies report recommended that "[t]he federal government should develop and regularly update an IT R&D roadmap for disaster management with the involvement of a full range of stakeholders."[22] The Academy report identified six key areas of IT-enabled capability in which shorter-term development and longer-term research offer the potential for significant benefits:

- More robust, interoperable and priority-sensitive communications;
- Better situational awareness and a common operating picture;
- Improved decision support and resource tracking and allocation;
- Greater organizational agility for disaster management;
- Better engagement of the public; and
- Enhanced infrastructure survivability and continuity of societal functioning.

An additional report from the Federal Communications Commission highlighted that "broadband communications applications could offer the public safety community a number of benefits, including video surveillance, real-time text messaging and e-mail, high resolution digital images and the ability to obtain location and status information of personnel and equipment in the field."[23] In particular, Congress directed the FCC to analyze whether the public safety community needed more spectrum and, additionally, if the development of a nationwide public safety communications network would resolve the problems raised by the performance of existing public safety systems during disasters from 2001-2005. The FCC's 2005 Report back to Congress found that emergency response providers would benefit from development of "an integrated, interoperable network capable of delivering broadband services nationwide."[23] The Commission proceeded to design a single national license for public safety broadband frequencies in the 700 MHz band for the Public Safety Spectrum Trust (PSST) (a non-profit organization composed of representative public safety and local government organizational representatives). The 700 MHz D-block broadband strategy was in addition to 50 MHz previously allocated by the FCC to public safety in the 4.9 GHz band.

Finally, a comparison of three "requirements" documents related to public safety reveals some important consensus – as well as some important diversity – concerning the direction that a research and development roadmap for advanced networking should take.

One, the PSST released the *Information for Bidders on a National Public Safety Broadband Network* in 2007 [17]. This document contained a number of requirements for what was perceived at the time to be a single, national broadband public safety network.[9] These were in large part derived from other sources: (i) the Project MESA Statement of Requirements, which is an ongoing effort to work with the international telecommunications industry to define mobile broadband data requirements [29]; and (ii) the SAFECOM Statement of Requirements released in 2005, which defines voice, video and data requirements of local first responders and incident command [14].

Two, the first of these sources, the Project MESA Statement of Requirements, states that it [29]:

> reflects the vision of a mobile broadband network (shared and/or *ad hoc*) that can be simultaneously accessed by multiple users, using various applications and levels of security, in a specified geographical area, and that may operate potentially independently from the availability of public networks and the supply of commercial electrical power . . . Emphasis has been placed on those applications and technological platforms that current technology has not yet satisfactorily addressed.

The Project MESA Statement of Requirements explicitly recognizes the value of wireless technologies to provide both broadband and narrowband application support (e.g. voice and video), improve spectrum efficiencies, be frequency neutral, and incorporate frequency agility.

And *three*, the SAFECOM Statement of Requirements, in contrast, focuses on interoperability. It stresses the "ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions, some of which may use different technologies, infrastructures and/or frequency bands regardless of system including transitioning between commercial systems and private LMR systems."[14] Moreover, the SAFECOM Statement of Requirements provides use cases where public safety will need advanced capabilities, such as for sensor reading, streaming video, air-to-ground video and other situational awareness technologies. It further

[9] The network was to be constructed by a commercial carrier, who could use the same infrastructure to deliver commercial service and public safety service nationwide. In this paper, we will not address the failure of the commercial service provider model or the failure of the D-Block auction to attract a bidder at the reserve price.

anticipates *ad hoc* networking and certain network federating concepts. In spite of some of its forward looking perspectives, however, the SAFECOM Statement of Requirements also adheres to traditional view of siloed public safety spectrum allocations, private network architectures for public safety, and the concepts of exceptionalism. We return to SAFECOM's work and suggest an expanded vision for SAFECOM leadership in Section IV(C).

C. Trust Requirements for Public Safety

There remains a chasm between the advanced networking research community's vision for evolved communications and the support and information provided to public safety stakeholders "on-the-ground." While the research community may be ready to embrace frequency agility and spectrum sharing, public safety practitioners typically resist network or infrastructure sharing, claiming that their requirements for reliability and coverage are simply too different from all other wireless users to justify the inherent risks of losing control of aspects of networks which support first response [24].

Further, there is skepticism among public safety practitioners as to whether a trusted prioritization scheme can be developed to reliably pre-empt non-public safety uses when public safety needs spectrum. In addition, several characteristics are insisted upon. There is an insistence that emerging technology must be backward compatible with legacy narrowband push-to-talk networks, and that legacy narrowband push-to-talk applications are not necessarily "just" applications, but that they are the mission critical network design cornerstone (and all other applications have to ride along or ride separately). There is insistence that there must be "public safety" standards authored and controlled by public safety (which, to date, bear limited resemblance to commercial standards). There is a cultural insistence that public safety must own its own infrastructure and spectrum, and that it should be owned by local or state users. This is often done city-by-city and even agency-by-agency. Exclusive ownership equates to control. Traditionally, this exclusive form of control is the only one trusted when first responders' lives are on the line.

Consequently, a critical need for the smart radio development community is to introduce technology innovation that can meet the *capability* requirements for public safety advanced networks while still accommodating the public safety community's *trust* requirements. Specifically, collaboration must allow agencies to retain control over essential aspects of the network they use. The diversity of first responder organizations and the local governments who operate them dictates that *local control* must be embraced by any successful cognitive radio architecture. As explained in Section IV, we propose that the catalyst to make smart radio a preferred technology will be innovations in software policy controls and administration. Smart radio architectures provide a

technological way to gracefully migrate the public safety community from distrust to trust. Before examining the potential of smart radio architectures, however, in Section III we next address the organizational behavior difficulties involved in more extensive inter-organizational communications.

III. SURMOUNTING RISK IN INTER-ORGANIZATIONAL COLLABORATION

Section II explained that extensive collaboration is necessary to meet next generation advanced public safety requirements. Even as technological innovation makes such advanced capabilities feasible, however, the migration towards advanced networking architectures will be challenged by a host of non-technical factors. The public safety community is composed of thousands of independent agencies which hold spectrum licenses and have sunk considerable resources into their own expensive land mobile radio (LMR) infrastructures. Asynchronous budget cycles across agencies make it unlikely that these agencies could in lock step afford a "big bang" simultaneous change of technological direction [4].[10] Moreover, the prevailing product roadmap for LMR systems continues to be P.25, a technical standard which has only proven to be partially effective but nonetheless directs the development of many public safety systems.[11] Finally, although enabling technologies (like cognitive and software defined radio, discussed further in Section IV(A) *infra*) present significant advantages for the public safety communicator, policy incentives are lacking which would strongly motivate these thousands of communities and their vendors to move in consort toward a new future based on advanced technology developments.

As we explain in this Section III, inter-organizational collaboration is hard. The tenacity of non-technical barriers inherent in meaningful public safety collaboration – including sharing and federating – makes cooperative objectives particularly difficult to quickly achieve. Part A identifies that collaborative efforts require that an agency (a "trustor") assume the risk of trusting another agency (a "trustee") (i) to act in good faith and not act opportunistically, and (ii) to be able to competently complete obligations

[10] In contrast to traditional LMR systems, the 700 MHz "D-Block" provides hope of offering greater simultaneous uniformity to public safety broadband data communications. As noted above, however, the future of the D-Block is unclear at this time following the failed 2008 auction [47].

[11] P.25 stands for the Association of Public-Safety Communications Officials' ("APCO") Project 25. APCO and the Telecommunications Industry Association ("TIA") are collaborating on developing a suite of "standards" for public safety land-mobile radio, including over the air interfaces and other standards that are being adopted for next generation systems, but only by the public safety user community. Concerns about the efficacy of P.25 standards – ranging from incompatibility between vendors to cost – has been articulated elsewhere [53].

assumed as part of the collaboration. Crucial aspects of relationships such as trust and risk must be addressed in order to make successful cooperation possible. Next, Part B identifies strategies for building confidence and trust in collaborative relationships. Finally, Part C develops a framework of hazards which threaten public safety collaboration. Case studies illustrating these hazards are included.

A. Trust and Risk in Collaborative Ventures

Reluctance to cooperate across agencies is not merely a matter of recalcitrant public safety agency leaders' stubborn adherence to legacy modes of thinking. A wide range of non-technical factors conspire to make public safety collaboration difficult. In this Part A, we focus on the critical considerations surrounding the roles of *trust* and *risk* as affecting the behavior of organizations contemplating a collaborative venture.

Cooperative relationships by definition involve one or more partners and are predicated on the participants' decision to collaborate rather than pursue their respective objectives alone. Collaborations are a "particularly risky ventures, so some trust is required to initiate them."[26] Collaborative advantage is achieved where two or more entities cooperate such that the public benefits of cooperation exceed the costs.

Literature on inter-organizational collaboration illustrates that a reluctance to cooperate is hardly unique to the world of public safety and, moreover, a leader's skepticism concerning collaboration may be a rational decision given ample evidence that "collaboration imposes huge demands on those entering into it and that the likelihood of disappointing outputs and failures is high."[26],[27] Part of the challenge involves the "typically ambiguous, complex and dynamic structure of collaborations."[26] In addition to myriad tangles and costs inherent in partnering with others, a problem of *embeddedness* amplifies the risk of failed cooperation [27]. Exiting a flailing inter-organizational relationship can be precarious because partners are often entangled with one another as a result of their cooperation. For example, if two public safety agencies share LMR infrastructure such as towers and equipment on towers, exiting the relationship could mean that one of the collaborative parties lose access to critical infrastructure. Plainly put: achieving successful and meaningful collaboration is hard and the consequences of failure can linger after the collaboration dissolves.[12]

Trust and *risk* between partners are crucial dimensions of inter-agency cooperation. But what is meant by trust and risk has not been fully explored, particularly in the context of next generation public safety

[12] An additional drag on innovation could be that public safety agency decision-makers are generally "risk-averters" who tend to overestimate the probability or magnitude of losses [30]. This is an empirical proposition which would make for an interesting study. That is, do leaders and technology decision-makers in public safety agencies tend to be risk-averse and, therefore, have a lower general risk propensity than other decision-makers?

communication architectures. When examining inter-organizational collaboration, the fields of psychology, economics, sociology and organizational sciences recognize the vital role of trust [26],[28].[13] Moreover, empirical research on collaborative relationships reflects that – not surprisingly – practitioners view trust as "an essential ingredient for successful collaboration" and that trust is often perceived as lacking in their own collaborations [26]. "Words such as *hostility*, *fighting* and *mistrust* are frequently used." [26] Commentators have noted that trust is not meaningful without elements of uncertainty and risk [31]. Risk entails vulnerability when a trustor depends on a trustee to fulfill its responsibilities to the collaborative venture [26]. Yet, public safety organizations are notoriously risk-averse when it comes to "trusting" an outside agency with operational control which might put their first responders in jeopardy.

Significantly, from the perspective of the trustor, perceptions of trust and risk each concern "the same underlying construct of probability estimates" concerning the behavior of the trustee in a collaborative venture [30]. That is, perceptions of trust and risk reference the same set of probabilities concerning whether a trustee will fulfill its obligations and responsibilities. Subjective trust refers to a trustor's beliefs about the likelihood of the trustee *fulfilling* its obligations and responsibilities. Meanwhile, perceived risk refers to a trustor's beliefs about the likelihood of the trustee *failing to fulfill* its obligations and responsibilities. Accordingly, trust and risk reflect opposite sides of the same coin. Another way to put it is that while trust and risk represent "contrasting mentalities," such mentalities represent "mirror images of each other."[30]

Researchers T.K. Das and Bing-Sheng Teng sort a trustor's probability estimates concerning a trustee's behavior and capabilities into two broad categories: (1) good faith, and (2) capability [30]. Figure 1 below represents a simple view of this conceptual arrangement.

Trustee Good Faith Considerations		**Collaboration Capability Considerations**	
Goodwill Trust	**Relational Risk**	**Competence Trust**	**Performance Risk**

[13] This is not to say that trust is entirely understood or agreed upon. As one commentator has colorfully put it, "trust . . . tends to be somewhat like a combination of weather and motherhood; it is widely talked about, and it is widely assumed to be good for organizations. When it comes to specifying what it means in an organizational context, however, vagueness creeps in." [31] Similarly, other commentators have opined that trust "is one of the most frequently used and yet least understood of significant concepts in the social sciences." [30]

Figure 1: Conception of Trust and Risk Categories Affecting Trustor's Perception.

The first category, *good faith*, is composed of goodwill trust and relational risk, which are the flip sides of one another. "Goodwill is the trustor's belief about the trustee's intention as well as his willingness to act in the interests of the trustor."[30] Meanwhile, relational risk is the inverse and concerns the incentive and ability of the trustee to behave opportunistically. While individually rational, opportunistic behavior – "or self-interest seeking with guile" – produces a "collectively suboptimal outcome."[27]

The second category – *capability* – is composed of competence trust and performance risk. Similar to goodwill trust and relational risk, competence trust and performance risk are also mirror images of one another. Competence trust reflects the notion that, assuming good faith participation, collaborative obligations and responsibilities can be discharged by a party (or the parties together) given technical skills and other capabilities. "Competence trust is the probability that the trustor believes the trustee has the necessary skills and abilities to carry out certain actions and achieve desired results."[27] Performance risk is the inverse: it concerns a perceived *inability* of a trustee to perform even where the trustee acts in good faith.

As we elaborate upon in Part B, understanding the looping nature of trust and risk is crucial in developing successful collaborative relationships.

B. Trust-Building Loops and Formation of Confidence

Collaborative projects involve a cyclical feedback process whereby trust and risk within a relationship are enhanced or diminished over time. Circles – both "virtuous" and "vicious" – and loops are commonly invoked to describe the iterative and reinforcing nature of trust involved in collaboration [26], [30]. Rather than a static factor, trust is more accurately understood as a "dynamic phenomenon" associated with "a series of reinforcing processes that characterize collaborative relationships."[37] Additionally, studies indicate that seemingly inconsequential factors at formative stages can strongly influence trust (or lack thereof). In this respect, *path dependent* properties affect trust in relationships insofar as early and unexpected events help determine the end state [37].

Given the difficulties involved in achieving collaborative advantage, it is understandable that public safety officials are often resistant to inter-organizational cooperation. Confidence in partner cooperation is required for any entity to voluntarily enter into an inter-organizational relationship.

Academic work provides insight into requisite levels of confidence necessary to induce collaboration between entities, as well as how such requisite levels of trust can be developed [27],[30]. *Confidence* may be defined as an entity's perceived level of certainty that a partner in a cooperative relationship will pursue mutually compatible interests (rather than act opportunistically) and, furthermore, the level of certainty that collaboration *can* achieve the mutually compatible goals which are sought [27],[30].

The minimal level of confidence in partner cooperation required for any entity to voluntarily enter into an inter-organizational relationship will vary with the circumstances. Notably, the requisite degree of confidence required to enter into a cooperative relationship is higher where the stakes associated with possible outcomes are significant, while lower degrees of confidence are needed where the stakes are reduced [27]. In addition to trust, control presents an additional mechanism which builds confidence in collaboration. By *control* we refer specifically to mechanisms which serve to enhance the *level of control* in a collaborative setting – *viz.*, the "degree to which one believes that proper behavior of the other party is ensured."[27] In inducing collaboration, the levels of *trust* and *control* each "jointly and independently contribute to the level of confidence in partner cooperation."[27]

Early initiatives which seek modest outcomes with low stakes are not just more likely to be entered into (because they require less confidence), they are also more likely to be successfully executed and, in turn, build trust and confidence between entities. Accordingly, where possible, an approach which builds trust and cooperative competency through incremental steps is preferred. "[T]rust needs to be developed in a conscious and gradual manner."[27] As part of this development process, trust is enhanced where cooperative parties identify and cultivate congruent purposes, values and expectations between themselves. This is achieved, however, only as a result of a "cumulative product of numerous interactions" which takes considerable time [37].

In addition to taking time to build, trust is fragile. The iterative and reinforcing nature of trust and risk – whereby failure in turn undermines trust – means that ambitious initiatives which go awry can quickly and perhaps irreparably damage relationships. "Empirical and theoretical analyses of trust are consistent in pointing out that while building trust is a gradual process, it can be destroyed very quickly by single events or inconsistencies on the trustee's behavior."[37]

In catalyzing the expansive types of collaborative networks envisioned by the next-generation researchers and developers, the upshot of the literature on collaboration suggests that it is important to consider three questions: (1) What is the maximum operational benefit which could be

achieved while requiring a *low level of initial confidence* by a public safety participant? (2) What *trust building* mechanisms can be used to enhance goodwill and increase collaborative competence between public safety agencies? And (3) What *control* mechanisms can be used to increase confidence in the collaboration? We turn to these considerations in Section IV. First, however, we develop a framework of hazards that reflect trust and risk considerations for public safety agencies' communications collaboration.

C. Hazards to Public Safety Collaboration

A framework is lacking which connects the body of academic literature concerning risk and trust with issues specific to public safety communications issues.[14] We envision two purposes for such a framework. First, as a descriptive matter, the framework has explanatory value as to why federal, state and local public safety entities have found collaborative goals, such as interoperability, so difficult to meet. Second, at a practical level, public safety policymakers, officials, and contractors can use (and refine) this framework as a tool when considering development and expansion of next generation collaborative networks.

In Figure 2 below, we suggest five broad hazards arising from cross-entity collaboration based on our review of public safety case studies, literature, and other reports concerning public safety interoperability. The separate trust/risk categories of *good faith* and *capabilities* provide useful prisms for analysis of public safety communications collaboration. Each hazard represents a dimension of potential difficulties when one or more agencies cooperate with the goal of achieving communications collaborative advantage.[15]

[14] Two related studies [50],[51] concerning collaborative networks involving governmental entities illustrate the utility of such a focus. In [50], the researchers identified risk factors attendant to collaborative projects. Meanwhile, a companion project [51] focused on aspects of trust in collaborative projects. While helpful, the separation of trust and risk between the two studies do not highlight the connection between the concepts underscored in this paper (and results in some conceptual difficulties).

[15] The focus of this framework is on trust and risk factors. Future work may include control mechanisms as an additional tool to build collaborative confidence necessary to induce cooperation.

Hazard	Goodwill Issues for Public Safety	Capability Issues for Public Safety
Governance and Organizational Hazard that governance control mechanisms, administrative costs of coordination, ambiguous or misunderstood roles, and leaders' lack of coordination experience results in (i) opportunistic behavior by collaborative members; and/or (ii) ineffective execution of collaborative obligations.	Risk that under-definition of formal relationships – including enforceable rights and obligations among participants – results in opportunistic behavior contrary to the best interests of a collaborative effort. How do power imbalances between participants affect governance and control? Where larger parties have control, how constrain their ability to act opportunistically? How overcome free rider problems related to parties' contributions? (E.g., who leads the collaborative network? who pays for necessary management, leadership and administration?)	How train leaders to work collaboratively across organizations? How manage overhead and administrative costs associated with collaboration? How define roles and obligations in advance without knowing how collaboration will evolve? How spur collaborative best practices within agencies which are rarely designed to function within a collaborative environment?
Legal Hazard that that laws and regulations – existing or future – prohibit or have deleterious effect on the collaborative effort.	What remedy or consequences where a party fails to make a promised contribution and/or fail to fulfill an obligation? Where infrastructure is jointly created and/or shared, what happens to "right" to access infrastructure if a party withdraws from the collaboration?	How address FCC/NTIA regulations prohibiting sharing of public safety licenses? Where spectrum waiver is obtained, is there uncertainty of renewal or revocation of waiver?
Political and Funding Hazard that political considerations result in insufficient funding or changed incentives concerning participants' collaborative objectives.	Even where goodwill exists today, what if leadership changes (e.g., election of a new governor) and eviscerates support – and funding – for an agency's participation in an existing collaboration? Will "turf wars" between agencies affect the collaborative effort?	How achieve collaboration between two entities when funding and replacement cycles for equipment and radio systems are not synchronized?
Technical and Operational Hazard that a fundamental objective of the project cannot be fulfilled due to technical problems or operational difficulties associated with collaboration.	How guarantee that trustee will not use a disproportional amount of a shared resource? If spectrum is shared, how ensure that trustee will not use too much at expense of trustor How address principal-agent problems where it may be in an entity's (i.e., the principal's) overall interest to collaborate, but an individual manager's (i.e., the agent's) self-interest is to act in ways which undermine the collaboration?	How maintain a command and control hierarchy in an emergency situation where network and/or spectrum are shared? Danger that proprietary technologies frustrate open standards necessary to facilitate sharing between different networks. To extent command and control safeguards are built into a system (e.g., software), how allow for dynamic adaptability responsive to unique needs of situation?
Cultural Hazard that conflicts concerning language, behavioral norms, and organizational values will undermine cooperation.	Where behavioral norms and/or fundamental goals of agencies are incongruous, will divergence in incentives result in opportunistic behavior?	How get organizations to – literally – speak the same language? For example, where one agency's terminology during an emergency differs from another's terminology, how can these differences be managed?

Figure 2: Hazards of Public Safety Inter-Organizational Collaboration

Risk associated with these five hazards conspire to prevent collaborative public safety networks from emerging, and, further, even where collaborative efforts are launched, these hazards frequently hinder and sometimes prove fatal to cooperation. Illustrations from four notable public safety collaborative efforts – the Phoenix Regional Wireless Network and Trunked Open Arizona Network ("PRWN/TOPAZ"), the federal Integrated Wireless Network ("IWN") project between the Department of Homeland Security ("DHS") and Department of Justice ("DOJ"), the Alaska Land Mobile Radio System ("ALMR"), and the Nevada Shared Radio System ("NSRS") – underscore the hazards involved in public safety collaboration. While Arizona's collaborative efforts and the federal government's IWN have been derailed by the hazards identified in this paper, the successes in Nevada and Alaska demonstrate that with effective leadership and consistent concern for the cultural aspects of collaboration, these hazards can be managed. Indeed, the extensive scope of ALMR and the public-private nature of NSRS suggest that – even in the most complicated of collaborations – organizational hazards and "people-problems" can be overcome.

PRWN/TOPAZ: Governance and Political Hazards

Governance-related hazards soured a collaborative effort between the cities of Phoenix and Mesa. The State of Arizona, through the Public Safety Communications Commission, developed a long-term plan for a state-wide, collaborative, public safety network. In the short-term, the state emphasized deployment of a suite of interoperable radios (UHF, VHF and 800 MHz) as part of the Arizona Interagency Radio System ("AIRS") [32].

Phoenix and Mesa, the largest population centers in Arizona, together developed the most successful advanced public safety network in the state, a collaboration which was among the most progressive in the nation [48],[33]. The joint Phoenix Regional Wireless Network and Trunked Open Arizona Network ("PRWN/TOPAZ") was considered "a genesis or key building block for the statewide, interoperable, public safety radio system."[33] Indeed, the initial success of PRWN/TOPAZ was sufficient to induce medium and small-sized agencies to request permission to join the network, not only for improved interoperability, but also to serve as a day-to-day operability platform. In short, other agencies recognized the potential benefits of enhanced collaboration.

From the beginning, PRWN/TOPAZ system faced significant relational risks concerning governance and organization hazards. Founded by a handshake agreement, the PRWN/TOPAZ system lacked formally

defined rights and obligations [33]. When additional agencies asked to join the network, this provided impetus for Phoenix and Mesa to formalize their relationship. The prospect of sharing resources with new agencies required agreement concerning: (i) how to share costs, and (ii) a governance structure which would provide control mechanisms for the original two owners over the joint system. When the cities attempted to formalize their *ad hoc* collaboration and memorialize a governance structure for the network, however, disputes over control and funding arose between Phoenix and Mesa. Negotiation over rights and obligations led to tensions and, as a result, the cities are now moving forward with separate governance documents and systems. Most importantly, any continued success of the joint or shared PRWN/TOPAZ system hinges on its ability to revisit and overcome the governance impasse and repair strains related to friction between the entities.

More broadly at the state level, political hazards have been implicated by a change in the administrative body charged with oversight of public safety radio communications matters. Specifically, the Public Safety Communications Commission was transferred from the Department of Public Safety ("DPS") to the Government Information and Technology Administration ("GITA").[16] Historically, DPS generally managed public safety communications, including radio systems for state agencies. The long relationship between Arizona's public safety agencies and the DPS generated high levels of goodwill and competency trust: agencies knew that the DPS understood their needs and was capable of fulfilling them. This trust was instrumental to the PSCC's ability to initiate interoperability efforts and helped lay the foundation for the long-term interoperability plan. With the change in oversight to GITA, however, there is some concern that GITA and public safety agencies will initially have trouble communicating effectively, potentially eroding support for the long-range interoperability plan. Indeed, GITA is already pushing interoperability efforts in a different direction than that originally proposed by the PSCC, and some involved are concerned that state-wide support for interoperable public safety networks could wane [48].

Integrated Wireless Network: Funding Hazards

Federal agencies are not impervious to similar problems. For example, funding issues – among other hazards – have all but ended the Department of Homeland Security's ("DHS") and the Department of Justice's ("DOJ") collaborative effort to build the Integrated Wireless

[16] Much like Arizona, ALMR similarly faced significant political hazards when control over the state's participation in ALMR was bounced back and forth between two state agencies [7].

Network ("IWN"). As envisioned, IWN would have provided interoperable communication over a secure, wireless, nationwide communication network for over 81,000 federal agents and fifty states and territories [34].

As explained in [34], significant funding hazards associated with IWN yielded high levels of performance risk (and, conversely, low levels of competency trust). This is at least in part due to disparate funding mechanisms between DHS and DOJ. DHS has a flexible funding system that makes it better able to satisfy IWN and legacy maintenance needs. By contrast, funding for DOJ wireless technology is disbursed by the Wireless Management Office ("WMO"), which manages the consolidated budget for all DOJ components (the FBI, ATF, etc.). Compounding the problem, a DOJ component is only awarded funding to replace legacy systems if it demonstrates that the legacy technology is on the verge of failure. Thus, the DOJ cannot replace legacy equipment with IWN compatible technology across the board, but instead must wait for longer replacement cycles for equipment. The mismatch in funding and replacement cycles resulted in high levels of performance risk and helped undermine the opportunity to create an integrated wireless network.[17]

ALMR: A Case of Dynamic Leadership Structure

The Alaska Land Mobile Radio System ("ALMR") is a sweeping collaborative effort between federal, state, and local agencies to provide Alaska with three types of interoperability: day-to-day, mutual aid in disaster, and task force interoperability [7]. ALMR achieves interoperability by pooling spectrum between both state and federal users and by sharing infrastructure. While impressive for its success in achieving collaborative network capabilities, however, the ALMR System has not been immune to the hazards detailed above. Governance and leadership issues perhaps posed the greatest hazard for ALMR and, indeed, one of ALMR's most impressive achievements have been its ability to address such hazards through leadership structures which have met the project's needs.

[17] Moreover, even if funding and replacement cycles matched, additional funding hazards would remain due to insufficient overall funding. Between Fiscal Year 2000 and FY 2006, $772 million was allocated to the DOJ WMO. The DOJ estimates, however, that even if IWN is not implemented it will need more than $900 million to replace existing legacy equipment. Though funding is expected to increase, DOJ officials expect to receive only fifty percent of requested funds and are concerned that, without an immediate and drastic increase in funding, IWN will fail [34]. Despite an agreement DHS and DOJ would submit a joint budget report (an action which the entities complied with from 2005-2007), the two agencies submitted separate budget reports in 2008. This is a strong indicator that the DHS and DOJ are no longer working toward a cooperative interoperability solution. Moreover, DHS is now pursuing small, localized networks without the help of DOJ. Indeed, the DHS refuses to re-define the collaborative relationship without a promise of independent contracting rights with the IWN suppliers [34].

From the outset, ALMR's ambitious scope created perceptions of performance risk, as members were naturally skeptical at various stages of the project that such an ambitious undertaking could be completed. ALMR leaders responded by creating a strong Executive Council to secure buy-in from key stakeholders. The Executive Council was led by four members, one representative each from the Department of Defense, non-military federal users, state agencies, and local users. Each member had equal standing despite the fact that the Department of Defense paid for a disproportionate amount of the build-out. Indeed, the Executive Council served as a face of legitimacy for the project during its formative years and sufficiently increased goodwill and competence trust among member agencies, making them more comfortable with such a daunting collaboration. Additionally, the Department of Defense's presence as the champion of ALMR significantly lowered the perception of performance risk among collaborative partners during the network's build-out phase.[18]

NSRS: Bridging Cultural and Technical Hazards

Like ALMR, the Nevada Shared Radio System ("NSRS") is striking in its ambition. In particular, NSRS features collaboration between public safety agencies and non-public safety entities. The public-private collaboration includes public safety, the Nevada Power Company ("NPC"), the Sierra Pacific Power Company ("SPPC"), and the Nevada Department of Transportation ("NDOT") [55]. Operating in the 800 MHz range, the system provides interoperable coverage over the jurisdictions of both power companies and the state highway system.

From the outset, NSRS was characterized by high levels of goodwill and competency trust among partners and avoided many of the organizational hazards that trip other collaborative efforts. In this respect, NSRS is similar to ALMR, which similarly benefitted from high levels of pre-existing trust across organizations built over years of prior cooperation [7]. The original NSRS Memorandum of Understanding ("MOU") required each owner to build and maintain the infrastructure necessary to provide coverage to its jurisdiction [55]. Thus, each member had incentive (and responsibility) to fulfill its part of the collaborative effort. Aligning owner incentives and network incentives worked so well that the MOU was never legally enforced. As the system developed, and as trust built, owners not only maintained their own infrastructure but also began sharing surplus materials and labor across entities [55].

[18] ALMR also addressed risks for local first responders tied to perceived technical and operational hazards by lowering user's initial costs for involvement. Users were permitted to use the system cost-free as beta users while the ALMR network was being built out. This enabled ALMR to build some technical and operational trust during the build-out phase.

Despite its initial success in aligning owner incentives and group incentives, NSRS encountered governance and cultural hazards related to the public-private nature of the network. First, as the number of local users grew, the power companies (at least at their lowest levels of users and technical support) found it difficult to relinquish control over their infrastructure. Second, as the network became larger and more diverse, NSRS was plagued by inefficient flow of information between users. Both hazards, however, were addressed by hiring an outside manager – styled as a System Administrator. As an independent "enforcer," the new System Administrator was empowered to lead entities and individuals within the governance structure to comply with the needs of the network. Indeed, free of the entity-specific biases that would attend leaders of member entities, they System Administrator could focus on advancing the interests of the network as whole (and thereby alleviate principal-agent problems on a network level) [55].

The Systems Administrator not only aligned incentives within the network, he also reduced cultural hazards of collaboration, reduced relational risks and increased goodwill and competency trust among members by facilitating flow of information between agencies. Different agencies speak different languages and, at times, miscommunication led NSRS partners to defend their own positions rather than pursue effective collaboration. Understanding that effective communication is achieved between counterparts within organizations, the Systems Administrator acted as a go-between and drastically improved communication by bringing people together. Improved communications reduced perceptions that other agencies were unable to fulfill their part of the collaborative effort and diminished cultural hazards within NSRS.

IV. HOW COLLABORATIVE PUBLIC SAFETY NETWORKS CAN BE FACILITATED BY SMART RADIOS

Hazards endemic to public safety collaboration – as seen through the prism of trust and risk as well as existing collaboration case studies – suggest that policymakers must actively promote strategies designed to overcome non-technical barriers in order to achieve extensive cooperation. Policy-based networks using "smart" radios can and should be part of building trust loops necessary to lead public safety toward network federation and spectrum sharing. To be clear, smart radios alone will not resolve all collaborative hazards. However, even given today's public safety LMR landscape – *i.e.*, balkanized radio systems, cultural differences between agencies, frequency assignment patchworks, a dual spectrum management by the FCC and NTIA, and slow funding cycles – smart radios do not reinforce silo-based physical network separation, and instead enable a

migration toward collaborative advantage in a federated, policy-based wireless architecture.

This Section IV proceeds in three parts. First, the defining characteristics of smart radios as well as current public safety deployments of smart radios are addressed in Part A. Next, Part B proposes ways policy makers and researchers can develop and nurture trust loops and control mechanisms in the evolution of smart radio in order to spur willingness to enter into collaborative relationships. Finally, Part C discusses the importance of leadership by policymakers to help shape both awareness and willing participation in changing the paradigm for public safety networking.

A. Characteristics of Smart Radios

The existing and future capabilities of smart radios are set forth elsewhere [38]-[39], and it is not this paper's purpose to conduct extended technical examination. It is important, however, to highlight the most noteworthy smart radio characteristics which could create confidence in federated networking by managing risk for public safety communications. These have been discussed recently by Jesuale and Eydt in [39], from which Figure 3 below is reproduced.

Now	Future
Stovepipes Users are divided into different classes of eligibility and then assigned frequencies available only to that class. Users in different classes can't easily interoperate. Some users are desperate for more channels while neighboring spectrum is unused.	**Pools** Existing allocations are combined to give each user access to a broader range of spectrum. Users in different classes can communicate with each other on common frequencies as needed.
Fixed Frequency Assignments Users obtain licenses for exclusive use of certain frequencies, regardless of how often they use them.	**Dynamic Access** Users can access spectrum without a license when it is unused. Spectrum isn't left fallow just because it's "reserved."
Owner Operators Public-safety grade reliability is achieved by owning and operating all radio infrastructure.	**Shared Infrastructure** Collaborative or outsourced management of databases, routing, switching, authenticating and provision would negate the need for billions of dollars of duplicated facilities across the nation.
Single Network Access Generally roaming from one mission-critical network to another is not possible.	**Roaming** Radios can detect available channels and roam from band to band and network to network.
Narrowbanding Current mandate for VHF/UHF licensees to migrate to 12.5-kilohertz channels and then potentially to 6.25-kilohertz channels. The requirement forces users with broadband needs to higher frequencies with expensive buildout costs.	**Flexibanding** Users can negotiate both the bandwidth and the frequency band most appropriate for an application.

Figure 3: Developments Enabled by Smart Radios.

By smart radios we mean software defined radios ("SDR") and policy-based cognitive radios ("CR"). SDR utilizes software to implement flexibility and reconfigurability into radio device operation. In contrast to SDRs, "traditional radios feature designs that are fixed in a radio's hardware. Notably, SDRs allow much of what was previously done with hardware – including signal processing, modulation, and power control – to be accomplished in reconfigurable software."[3] In addition to enhanced flexibility, the central role of software in a SDR enables reconfiguration of devices and networks. "Reconfigurability is the capability of adjusting operating parameters for the transmission on the fly without any modification on the hardware components."[38]

Cognitive radios enable adaptable behavior based on a radio's environment. A CR is "a radio that is aware of its environment and internal state and alters its behavior based on that information and predefined objectives."[52] There are two notable aspects of cognition in a CR. One, a CR's *detection capabilities* allow it to be aware of its location and – with sufficient sensing capability – dynamically sense available and occupied channels across a range of frequencies. Two, CR is *policy-based* insofar as it relies upon machine-readable policies which direct whether the radio may operate given the circumstances [3]. Machine readable policies can reflect existing regulatory policies as well as other transmission constraints provided to the radio. Consequently, policies which render instruction concerning whether transmission is permitted, combined with the device's external awareness of its location and environment, provide the signature capabilities of a CR.

It is the cognition-like features of a CR which enable a radio to take advantage of SDR flexibility [54]. In this respect, the operation of smart radios is not governed by hardware and infrastructure. Rather, ***policies are the architecture*** for smart radios insofar as machine-readable policies provide the defining attributes concerning how radios operate (or not) given the broader constraints of a system's infrastructure. Unlike a static architecture where the operational characteristics are largely coterminous with hardware's constraints, the architecture of a smart radio system can be dynamically altered and reconfigured over time.

Smart radios are increasingly deployed in military environments and are no longer the exclusive province of laboratories and academic papers [2]. Additionally, devices with smart radio characteristics are also already playing a role in collaborative public safety communications. The Department of Homeland Security provided Thales with $6.25 million to develop the Liberty radio, released in February 2008, which operates on public safety bands ranging from 136 - 800 MHz [2]. Harris Corp. also has entered the market with a radio, the Unity XG-100P, which operates over

the same public safety bands and is P.25 compliant [2]. Cost is a concern as these smart radios are roughly $5,000. But Shared Spectrum Company is working with M/A-COM on a radio that is dramatically more affordable, targeting a cost of $500 by end 2008 [2].

While we are unaware of any other studies focused on smart radio's ability to affect organizational behavior aspects of public safety collaboration, several investigations have more generally recognized the potential for smart radio technologies to benefit public safety communications. For example, the SDR Forum's Public Safety Special Interest Group (SIG) in April 2006 completed a comprehensive analysis based on responses to requests for information [41]. Other papers have similarly considered enhanced capabilities and risks related to smart radios and public safety [42]-[44]. More recently, the SDR Forum has focused on specific use cases for cognitive radio in public safety [56].

B. Strategies to Build Goodwill and Competence

Two important strategies should be used to facilitate public safety collaboration: (i) exploit the dynamic, cyclical and iterative nature of trust and risk by gradually (and gracefully) building trust loops which reinforce goodwill and enhance cooperative competence; and (ii) insert trustor control mechanisms in parallel with trust loops. This approach is consistent with literature which suggests that "deliberate *building of trust* and more *effective control mechanisms*" present "two distinct avenues that can (and should) be pursued simultaneously."[27]

To be clear, we believe that it would be ill-advised to mandate a rushed course of extensive sharing based on smart radio technology. Viewed through the organizational behavior lens, the case for early simple sharing steps is stronger than a policy course which rushes to exploit all behaviors and strategies. While smart radios promise to help resolve organizational behavior challenges in public safety, they simultaneously introduce new problems. For example, emerging technologies invariably introduce uncertainty and, not surprisingly, the reconfigurable nature of smart radios is often viewed with some suspicion (*i.e.*, what happens in the case of a malfunction? what if a malicious user reconfigures software in a way that causes harmful interference to authorized users? etc.). More broadly, dynamic spectrum access entails greater challenges because it relies on systems level processes – sensor readings, databases, communication with other devices, complex decision algorithms, etc. – to avoid interference [54].

It would be equally mistaken, however, if policy-makers were to fail to recognize the vital role that smart radios should perform as part of the migration path toward extensive collaboration. In particular, three opportunities created by smart radios should be a critical part of

implementing each of these strategies. Smart radios should be used to: (1) enable trust-building through graduated sharing by leveraging the flexible architecture enabled by policy-based radios so as to maintain local end-user control over the network in ways that current, static LMR architectures cannot; (2) utilize control mechanisms associated with software and reconfigurability; and (3) enhance trust by reducing perceptions of resource scarcity. Each of these three opportunities for smart radios are discussed below.

First, policy-based controls will enable the kind of local risk mitigation required by a public safety agency. Cognitive radios, following machine-readable software policies that are updatable, provide public safety emergency response with significant levels of local control over the technologies' operational parameters. Indeed, it is these policy-based software controls which we view as a fundamental catalyst for inter-organizational collaboration.

To grasp this, it is important to distinguish between smart radio capabilities *versus* the behaviors and networking strategies which exploit those capabilities. Use of software-based policies enables gradual sharing. Significantly, smart radios are often associated with dynamic spectrum access (a behavior) and spectrum pooling (a sharing strategy) [24],[45]. Conceptual confusion results if capabilities and behaviors are conflated. To be clear, SDR and CR reflect what a device and system is able to do. In contrast, dynamic spectrum access represents a *behavior* which strategically leverages those capabilities. Given challenges inherent in cooperation, even if smart radio networks enable extensive collaboration, only some of the capabilities will be utilized in the near term. However, as trust and collaborative competency are established, a smart radio makes long term migration to extensive collaboration possible because the policies are the architecture and such policies are updateable. Innovations in policy control and administration within smart radio architectures provide a graceful way to migrate the public safety community from distrust to trust when federating in order to use applications and infrastructure that they do not necessarily own.

For instance, policies which allow public safety organizations to "roam" on each other's systems – using their frequencies when they are "in the area" – would be a small step forward and could provide near-term benefits. This cooperation would dovetail with mutual aid agreements that already exist between first responders in many areas. Indeed, smart radio policies could enable greater control insofar as written agreements between organizations – such as mutual aid agreements, memoranda of understanding, and standard operating procedures – could be embodied within machine readable language. Over the longer term, machine-readable language concerning the command structure at an event – such as National

Incident Management System ("NIMS") protocols – might be reflected in software policies as well.[19] To be sure, significant work remains to enable this level of intelligence. It is, however, an application which will provide public safety trustors important control within collaborative relationships.

Second, particularly in view of the long life-cycles of public safety devices which often leave first responders utilizing equipment that is outdated by several generations, reconfigurable public safety devices have great potential. This capability raises the tantalizing prospect of enabling updates to devices and networking techniques without requiring wholesale replacement of hardware devices [3]. Additionally, reconfigurable radios could switch from high bands (*e.g.*, 800 MHz) to low bands (*e.g.*, below 200 MHz) when they need to operate in tunnels or forests where propagation characteristics could be exploited, or repeater infrastructure does not exist. Finally, reconfigurability further reduces risks associated with embeddedness. In particular, policies can be changed or even rolled back during periods of distrust or following dissolution of a collaborative network. Along these lines, federal policy leadership must work with stakeholders to identify gradual collaborative strategies which exploit reconfigurability. Smart radios can play an important role in this migration because they open up the possibility that more advanced policies developed for wireless operations (authentication, prioritization, incident specific operational policies, spectrum sharing policies, etc.) can be obeyed by the radios, and authored as well as updated by the user community to fit the geography, environment and situation. Devices which permit reconfigurable policies could be particularly significant for public safety inter-organizational collaboration. This would enable small initial sharing steps which, once trust is established, could be expanded by a policy changes over the longer term.

And *third*, smart radio networks can enhance trust in inter-organizational collaboration by generally reducing perceptions of resource scarcity. Risks associated with opportunistic behavior by partners are more pronounced where resources are deemed highly scarce. Some of the most vexing resource shortages in public safety networking have been licensable spectrum, affordable yet reliable equipment, and the ability to add broadband features and coverage of networks. For a public safety agency, collaboration is fraught with relational and performance risks when accompanied by shortages in spectrum, funding, capabilities and coverage.

In contrast, trust is easier to establish and maintain – and risk easier to

[19] NIMS enables responders across jurisdictions and disciplines to coordinate emergency response. "NIMS benefits include a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management." [49]

mitigate – in situations where both the trustee and trustor have ample resources sufficient to maintain collaborative goals. Smart radios offer the potential to create abundance (or at least efficiencies) in spectrum, reduce the reliance of public safety on expensive infrastructure to create coverage, and reduce the cost of end user devices by taking advantage of commercial economies of scale. Abundance breeds confidence by reducing risk of shortage. The case studies of Alaska's ALMR, Nevada's NSRS, and Arizona's PRWN/TOPAZ each reflect a willingness to initiate collaboration in order to collectively expand resources. In each of these systems, the risks of opportunistic partner behavior were diminished by the prospect of greater assets available to first responders.

C. Federal Leadership to Initiate the Collaborative Paradigm

Trust loops promoted by public safety radio architectures should result in a more unified future vision of advanced architectures. Moreover, as discussed above, this approach could be calibrated with the needs of public safety agencies so as to enable local control and graceful migration. In order to avoid several more years of constrained public safety communications capabilities, however, attention must now focus on advancing the vision and knowledge base of state and local practitioners.

To be sure, much progress has been made by the public safety community to address both interoperability and funding shortages through the development of shared wireless networks. Promising developments so far are oriented around shared and trunked LMR systems[20] with inclusive governance structures, the development of Regional Planning Committees ("RPCs") to develop band plans for public safety spectrum, and the development of State Interoperability Executive Committees ("SIECs") which set strategic statewide direction for federal grants from the DHS. Nonetheless, future efforts must be expanded past the borders of traditional private LMR frameworks. State and local responders must know about advanced federated networking architectures – *viz.,* what they are, when they are coming, and what impacts are likely. A bridge should be created between the ITFAN advanced research agenda for federal agencies and the current DHS standards and best practices articulated for state and local emergency response communications networks.

Two notable programs within the federal government which provide

[20] 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.

direct leadership on technology trends to the public safety communications community could serve as this bridge between federal research and the public safety communications agenda. *One*, the National Institute of Justice Communications Technology ("NIJ CommTech") [46] program is actively working to bring demonstrations of advanced network technology, specifically next generation development, to the public safety community. These types of demonstrations are vital to moving the community more toward acceptance of a new network framework that is not based on the limitations of the existing network architectures and spectrum policies.

Two, the SAFECOM program can exercise important leadership. SAFECOM introduced the SAFECOM Continuum in 2005 to "serve as a tool for urban areas working to improve emergency response communications interoperability."[21] This Continuum has since become a trusted paradigm for strategic change within the public safety community. In particular, it illustrates a baseline structure for local jurisdictions to measure their interoperability goals against an optimum level of interoperability. The SAFECOM Continuum has five "lanes" in which active local efforts will contribute to enhanced interoperability. These lanes are (1) governance, (2) standard operating procedures, (3) technology, (4) training and (5) usage. According to the Continuum, maximum interoperability is achieved when LMR systems are shared, governed collaboratively, used daily, and incorporate standardized operating procedures and continuous training and exercises. These efforts essentially create trust loops and the Continuum has been widely cited as a valuable guidepost for interoperable public safety communications.

Significantly, the Continuum could be extended to chart an advanced networking roadmap of collaborative strategies that we suggest are necessary. We have created a first version of an extended Continuum in Figure 4 below. The solid vertical line in the Extended Continuum denotes where the Continuum ends today. We extend the Continuum the right of this line. Our extension is intended to engage the current public safety conversation even as we advocate change to an architectural paradigm of extensive collaboration.

Interoperability Continuum
Extended for Next Generation Communications Capabilities

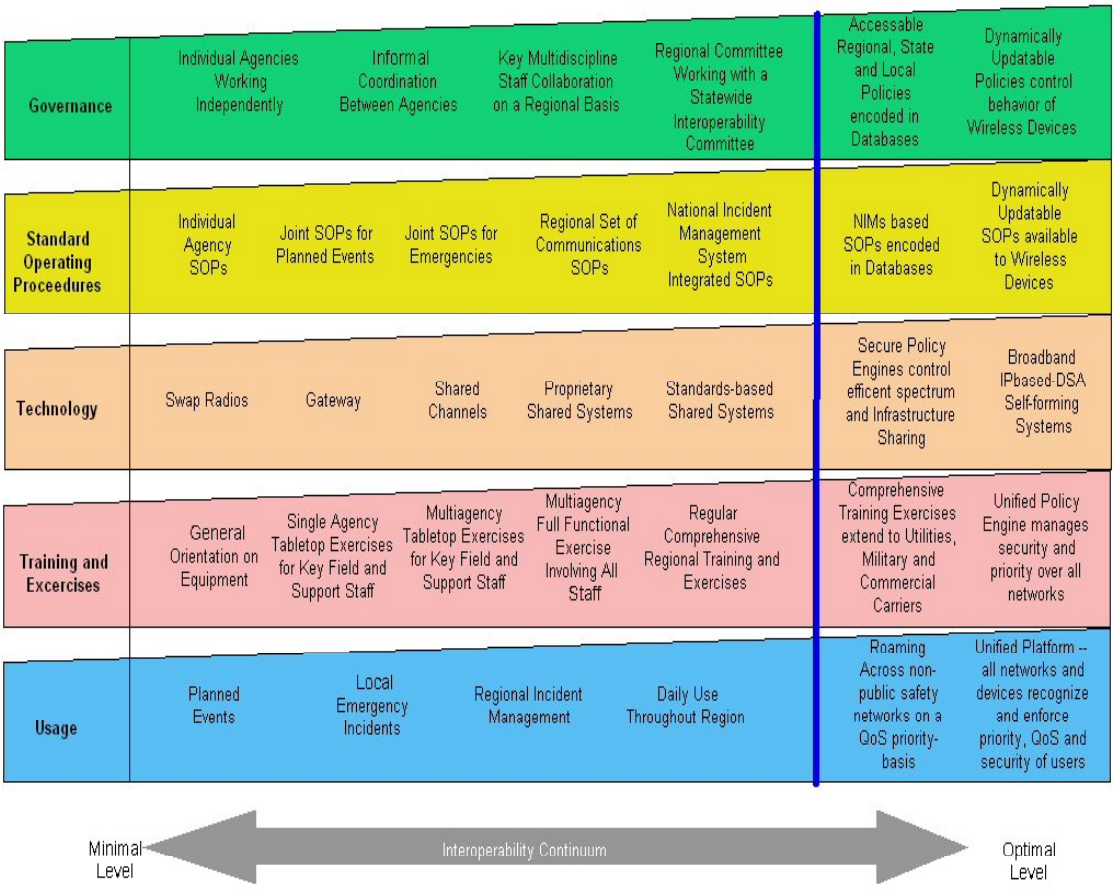

Figure 4. SAFECOM's Interoperability Continuum extended to include advanced networking architectures

The SAFECOM Continuum to date has attempted to layer interoperability upon legacy technological architectures and practices. In the extended vision presented in Figure 4, the paradigm changes to a flexible, federated, shared policy-based network architectures. An extended Continuum would provide vision and political support to the thousands of public safety communications network managers who must ultimately take the risks, negotiate the partnerships, commit the resources, and achieve the benefits of advancing these networks for first responders. Moreover, extending the Continuum's ribbons so as to reflect an agile, secure, federated, dynamic and self-forming network vision also tracks the existing federal research roadmap, such as the ITFAN report. In this respect, together with the NIJ CommTech program, the SAFECOM program could align with federal research efforts to play a key role in the advancement of policy based smart radio architectures.

V. CONCLUSION

Local first responders' communications systems are the foundation of public safety capabilities in emergencies and disasters. Yet, even as measured against certain commercial capabilities generally available to the public, first responders have fallen behind. Federal research increasingly recognizes the overwhelming benefits associated with collaboration. But to date the local and state first responder and emergency management community are neither fully engaged in setting the research agenda, nor are they realizing the fruits of research pointing toward extensive collaboration. Policy-makers should immediately begin advancing the vision and knowledge base of state and local practitioners concerning what advanced federated networking architectures are and what impacts are likely.

Before realizing the salutary effects from advanced networking collaboration, however, formidable non-technical obstacles must be squarely addressed. While resolving organizational behavior problems alone is not sufficient for successful public safety communications, it is a necessary and often underappreciated part of successful technology policy. Indeed, failure to embrace technical solutions amenable to a viable organizational behavior strategy will result in the loss of money and inadequate systems.

A better understanding of organizational behavior challenges

implicated by public safety cooperation is needed. Of course, inter-organizational collaboration problems are not unique to public safety. In other areas, "[m]uch research has been directed at gaining an understanding of the challenges facing those involved in interorganizational collaboration."[26] Significantly, important dimensions of public safety's collaboration travails are shared with other inter-entity cooperative efforts and public safety analyses should build on existing research. This paper highlights that insights from existing literature can be mined and, where appropriate, deployed to achieve an advanced public safety architecture.

Our analysis of existing literature suggests that thoughtful policy should identify ways to facilitate trust-building strategies such as the one articulated by [26]:

> [T]he trust-building loop aligns itself well with a 'small wins' approach within which trust can be built through mutual experience of advantage gained via successful implementation of low-risk initiatives. Trust can be developed over time moving gradually toward initiatives where partners are willing to take greater risks because a high level of trust is present.

Federal policy leadership must work with stakeholders to identify gradual collaborative strategies which enhance trust and control, resulting in greater confidence and more extensive collaboration. Smart radio capabilities can enable early sharing opportunities without relinquishing undue amounts of local control. Further, the reconfigurable aspects of smart radios do not lock in silo-oriented architectures going forward. As trust and confidence is enhanced, greater collaboration can be achieved by changing the policies which govern radio operation. To help galvanize progress, policy-makers might consider whether pilot areas of collaboration using policy-based smart radios can be created to serve as a model and a testing ground for advanced architectures.

More broadly, future research is needed concerning non-technical obstacles to advanced public safety communications. Organizational behavior and smart radios must be viewed in perspective. On the organizational behavior side, the challenges addressed in this paper – trust and risk across different hazards of collaboration – are certainly not the only major policy impediments. Funding insufficiency, timing of funding cycles across organizations, difficulties associated with public safety internalizing equipment costs but not spectrum costs, and how dual spectrum management between the FCC and NTIA affects public safety radio policy are critical (if obvious) areas for investigation.[21]

[21] Specific to funding necessary to achieve a next generation architecture, existing pressures and priorities may need to be addressed. For example, to start the migration path, a public safety agency

Research is also needed concerning less obvious barriers. Future investigation should consider, for instance, the existing incentive system of public safety agency managers with respect to procurement of information technology and radio systems. Analysis should examine the decision-making processes for public safety radio system purchases (*viz.*, who is involved, what rank the key decision-maker(s) has (have) in an organization, what information is provided to decision-makers, whether significant principal/agent issues exist, what the evaluation system is like for decision-makers, etc.). One might hypothesize that – particularly in the absence of market forces – punishments for a radio system's malfunction is far greater than rewards for procuring enhanced capability that did not exist before. To the extent that the weight accorded to possible harms unduly eclipse possible benefits of innovation, it may be necessary to alter incentives of managers so that outcomes are weighted differently.

Finally, on the smart radio side, our vision is as much a challenge to the development community as it is to policy-makers. Smart radios in general – and policy-based radios in particular – are catalysts for greater collaboration. But much work remains to be done. A major part of this work entails that, in order to realize smart radio's collaborative promise, architects of next generation systems must feature local controls which will accompany and enable the migration to collaborative public safety networks.

VI. AUTHOR BIOGRAPHIES

Brad Bernthal (303.492.0610, brad.bernthal@colorado.edu) is an Associate Clinical Professor at Colorado Law School in Boulder, Colorado, where he leads the Technology Law & Policy Clinic. Professor Bernthal also teaches as an adjunct professor in Colorado's Interdisciplinary Telecommunications Program. His doctrinal course offerings include Telecommunications Law & Policy and Spectrum Management. Prior to joining the Colorado Law faculty, Professor Bernthal served for two years as a Fellow with the Silicon Flatirons Center. His current research involves telecommunications policy issues with a focus on spectrum management and public safety. In February 2008, Professor Bernthal presented on public safety issues to the Commerce Department's *Spectrum Management*

must be willing to invest in an architecture and purchase equipment which will facilitate extensive sharing *before* such extensive sharing occurs. Such architecture and equipment will likely be more expensive than necessary to accommodate the immediate uses to which they will be put. This is because incremental collaboration through policy-based software controls is somewhat like a governor on a motor: capabilities enable more, but controls are imposed such that capabilities are not immediately maximized. Incentives and support for longer term capabilities may be necessary.

Advisory Committee.

Nancy Jesuale (njesuale@easystreet.net) is the president and CEO of NetCity Inc. in Portland, OR, a telecommunications strategic planning consulting practice advising local and state government and industry on technology implementation and emerging technology. She holds a Master's degree in telecommunications management from the Annenberg School at the University of Southern California. Ms. Jesuale has been involved in telecommunications strategies for local government since 1984. She has been an appointee to the National Task Force on Interoperability and the Oregon State Interoperability Executive Committee. She is an appointee to the National Academy of Sciences committee on the role of information technology for disaster response, which is currently conducting a research study for the US Federal Emergency Management Agency and Congress on emerging technologies for disaster response. She is a past chair of the Public Technology Inc. Task Force on Information Technology and Telecommunications. She was the Director of Strategic Planning for Telecommunications for the City of Los Angeles, and the Director of Communications and Networking for the City of Portland.

VII. REFERENCES

[1] Don Tuite, *Radio Interoperability – It's Harder Than It Looks*, Electronic Design (April 24, 2008).

[2] Donny Jackson, "A Corner Turned," *Mobile Radio Technology*, May 1, 2008. Available at : http://urgentcomm.com/mobile_data/mag/radio_corner_turned/

[3] Brad Bernthal, Timothy X. Brown, Dale N. Hatfield, Douglas C. Sicker, Peter A. Tenhula & Philip J. Weiser, "Trends and Precedents Favoring a Regulatory Embrace of Smart Radio Technologies," *IEEE INT'L SYMPOSIUM on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, Apr. 17-20, 2007.

[4] David Boyd. *"Command, Control and Interoperability,"* May 9, 2008. Available at: http://www.iacptechnology.org/LEIM/2008Presentations/Command%20Control%20and%20Interoperability_Boyd.pdf

[5] Carl Kent Erwin and David Aylward , "Next Generation Inter-organizational Emergency Communications: Making Tangible Progress While Broader Efforts Continue," *Aspen Institute 2006*. Available at:

http://www.aspeninstitute.org/atf/cf/%7BDEB6F227-659B-4EC8-8F84-8DF23CA704F5%7D/Homeland_InteroperabilityReport.pdf

[6] Department of Homeland Security. "*National Emergency Communications Plan,*" July 2008. Available at http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf

[7] Brad Bernthal, Steve Robertson & Justin Turner. "Collaborative Networks and the Alaska Land Mobile Radio System," presented at *Telecommunications Policy Research Conference,* 2007. Available at: http://www.silicon-flatirons.org/index.php

[8] Michael Chertoff, Homeland Security Secretary, remarks at S & T Stakeholders Conference East, Washington D.C USA, June 3, 2008.

[9] Michael Chertoff, Homeland Security Secretary, remarks at The Tactical Interoperable Communications Conference, Washington D.C USA, May 8, 2006.

[10] The National Consortium for Justice Information and Statistics, National Interoperability Summit Proceedings, Austin, Texas USA, May 24, 2006.

[11] G. Edward DeSeve, Business of Government Magazine, Creating Managed Networks as Response to Social Challenges, Spring 2007. Available at http://www.businessofgovernment.org/pdfs/forum07.pdf.

[12] ITFAN Interim Report, Office of Science and Technology Policy, September 15, 2007. Available at http://www.nitrd.gov/advancednetworkingplan/ (last accessed March 15, 2008).

[13] ITFAN Federal Plan For Advanced Networking Research and Development Pre-Print Version, Office of Science and Technology Policy, June 2008. Available at http://www.nitrd.gov/ITFAN-preprint-061108.pdf ,(accessed August 17, 2008).

[14] The SAFECOM Program, Department of Homeland Security. "Statement of Requirements for Next Generation Public Safety Wireless Communications & Interoperability", *Version 1.0*, March 10, 2004. Available at:http://www.safecomprogram.gov/NR/rdonlyres/3FFFBFBA-DC53-440E-B2EF-ABD391F13075/0/SAFECOM_Statement_of_Requirements_v1.pdf

[15] Project MESA, Service Specification Group- Services and Applications; Statement of Requirements Executive Summary, 2005. Available at: http://www.projectmesa.org/MESA_SoR/mesa_sor_executive_summary.pdf).

[16] National Telecommunications Information Agency. "Spectrum Management for the 21st Century: The President's Spectrum Policy Initiative," March 2008. Available at: http://www.ntia.doc.gov/reports/2008/FederalStrategicSpectrumPlan2008.pdf).

[17] Public Safety Spectrum Trust, Letter of Harlin McEwan to Prospective D-Block Bidders, dated November 30, 2007. Available at: http://www.psst.org/documents/BID2_0.pdf).

[18] National Response Framework (NRF), U.S. Department of Homeland Security, January 2008. Available at: http://www.fema.gov/emergency/nrf/)

[19] Department of Homeland Security, National Incident Management System, U.S., March 1, 2004 .Available at: http://www.nimsonline.com/docs/NIMS-90-web.pdf).

[20] Incident Command System Review Materials (2005). Available at: http://www.training.fema.gov/EMIWeb/IS/ICSResource/assets/reviewMaterials.pdf).

[21] SAFECOM Program, Department of Homeland Security, SAFECOM Interoperability Continuum, Office of Science and Technology. Available at http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability_Continuum_Brochure_2.pdf) (last accessed August 17,2008)

[22] Ramesh R. Rao, Jon Eisenberg, and Ted Schmitt. "Improving Disaster Management, The Role of IT in Mitigation, Preparedness, Response, and Recovery", National Research Council of the National Academies, National Academies Press, Washington D.C.,USA, 2007.

[23] Study to assess the Short-term and Long-term needs for allocations of additional portions of the Electromagnetic Spectrum for Federal, State and Local Emergency Response Providers, WT Docket No. 05-157 at 13 – 26, published December 16, 2005. Available at www.fcc.gov.

[24] W. Lehr and N. Jesuale, "Spectrum Pooling for Next Generation Public Safety Radio Systems**,"** accepted for publication *in IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySpan), Chicago, IL*, Oct. 2008.

[25] A. Gorcin and H. Arslan, "Public Safety and Emergency Case Communications: Opportunities from the Aspect of Cognitive Radio," accepted for publication *in IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySpan), Chicago, IL*, Oct. 2008.

[26] Chris Huxam & Siv Vangen. "Nurturing Collaborative Relations", *The Journal of Applied Behav. Sci.* Mar. 29, 2003.

[27] T.K. Das and Bing-Sheng Teng. "Between Trust and Control: Developing Confidence in Partner Cooperation in Alliance", *ACAD. OF MGMT. REV., 23* at *491*1998.

[28] Laura Black *et. al.* "A Dynamic Theory of Collaboration: A Structural Approach to Facilitating Intergovernmental use of Information Technology", *Proceedings of the 36th Hawaii International Conference on System Sciences*, IEEE 2002.

[29] Project MESA, *Introduction to the Project MESA Statement of Requirements*, available at http://www.projectmesa.org/MESA_SoR/SoR.htm (last checked Aug. 21, 2008).

[30] T.K. Das and Bing-Sheng Teng. "The Risk-Based View of Trust: A Conceptual Framework", *Journal of Bus. and Psychol,* Fall 2004.

[31] Black *et. al.* at Section 3.2 (citing Sheppard & Sherman, *The Grammars of Trust: A Model and General Implications*, 23 ACAD. OF MGMT. REV. 422-438 (1998)).

[32] Public Safety Common. Common, Arizona Dept of Safety, Statewide Common. Interoperability Plan (2007).

[33] Public Safety Commc'n. Comm'n, Arizona Dep't. of Safety, Transit, Summer 2007.

[34] Audit Div., Office of the Attorney Gen., Dept. of Justice, Progress Report on the Dev. of the Integrated Wireless Network in the Dept of Justice, 2007. Available at: http://www.usdoj.gov/oig/reports/OBD/a0725/final.pdf.

[35] Robert Howk, "New Emergency Radio System Is Nation's First," Alaska Journal of Commerce, October 20, 2003.

[36] Luis Reyes, Anthony Cresswell, and George Richardson. "Knowledge and the Development of Interpersonal Trust: A Dynamic Model," *Proceedings of the 37th Hawaii International Conference on System Sciences, IEEE,* 2004.

[37] Peter Smith Ring and Andrew H Van de Ven. "Developmental Processes of Cooperative Interorganizational Relationships," *Acad. Of Mgmt. Rev., 19, 100,* 1994.

[38] Akyildiz, Lee, Vuran and Mohanty, "NeXt Generation/ Dynamic Spectrum Access / Cognitive Radio Wireless Networks: A Survey, 1 (Accepted for publication May 2006)," Science Direct. Available at : http://www.ece.gatech.edu/research/labs/bwn/radio.pdf)

[39] Jesuale, Nancy and Eydt, Bernard C, "Spectrum Paradigm Shift : Policy reforms and user innovation can bridge next-generation cognitive-radio technology's use in LMR spectrum," Vol.23, No.3, Radio Resource, *Mission Critical Communications,* April 2008.

[40] Glenn Bischoff, "Harris Debuts Multiband Radio for Public Safety," *Urgent Communications*, August 5, 2008. *Available at:* http://urgentcomm.com/mobile_voice/news/harris-multiband-radio-0805/index.html.

[41] SDR Forum, "Software Defined Radio Technology for Public Safety, (Approved April 14, 2006)", *Document SDRF-06-1-0001-V0.00.*

[42] A. Gorcin and H. Arslan, "Public Safety and Emergency Case Communications: Opportunities from the Aspect of Cognitive Radio, accepted for publication," *in IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN), Chicago, IL*, Oct. 2008.

[43] John Powell, "Cognitive and Software Defined Radio: A Public Safety Regulatory Perspective," *National Public Safety Telecommunications Council's Software Defined Radio Working Group*. Available at: http://www.npstc.org/meetings/Powell%20SDR%20Regulatory%20Perspective%20061404.pdf

[44] Qiwei Zhang, Fokke W. Hoeksema, Andre B.J. Kokkeler and Gerard J.M. Smit, "Towards Cognitive Radio for emergency networks,"

Book Chapter in Mobile Multimedia: Communication Engineering Perspective, Nova Publishers 2006.

[45] Dale Hatfield and Peter A. Tenhula, "The Potential value of Decentralized trunking as regulatory precedent for the Introduction of Dynamic Spectrum Access technology," *IEEE INT'L SYMPOSIUM on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, Ireland, Apr. 17-20, 2007.

[46] National Institute of Justice CommTech Program. Available at : http://www.ojp.usdoj.gov/nij/topics/technology/communication/ (accessed August 20,2008).

[47] *Statement of Commissioner Michael J. Copps:* En Banc *Hearing on Public Safety Interoperable Communications*, Brooklyn, N.Y. (Jul. 30, 2008) (statement of Michael J. Copps, Comm'r of Federal Commc'n Comm'n).

[48] Telephone Interview with Curt Knight, Executive Dir., Arizona Public Safety Commc'n Comm'n (conducted July 17, 2008).

[49] Federal Emergency Management Agency, National Integration Center (NIC) Incident Management Systems Division Home**.** *Available at* http://www.fema.gov/emergency/nims/index.shtm (last checked Aug. 21, 2008).

[50] Lise Préfontaine, *Risk Management in New Models of Collaboration*, 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). *Available at* http://www.ctg.albany.edu/publications/online/new_models/essays/risk.pdf).

[51] Sharon Dawes, *The Role of Trust in New Models of Collaboration,* Center for Technology in Government at University at Albany, SUNY (2003). *Available* at http://www.ctg.albany.edu/publications/online/new_models/essays/trust.pdf).

[52] IEEE P802.16h/D5 Draft Amendment, "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Improved Coexistence Mechanisms for License-Exempt Operation," March 2008.

[53] 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).

[54] John Chapin, "Impact of Software Radio and Cognitive Radio on Spectrum Management," Presentation, July 2008 (Boulder, Colorado). The authors also recognize the benefit of additional insights from Dr. Chapin in this paper.

[55] Telephone Interview with Mark Pallans, System Administrator, Nevada Shared Radio System (conducted June 18, 2008).

[56] Presentation, Fred Frantz, *Cognitive Radio Applications for Public Safety Communications* (May 19, 2008) (citing SDR Forum, *Cognitive Use Cases for Public Safety* (Volume 1)) (PPT presentation on file with author).