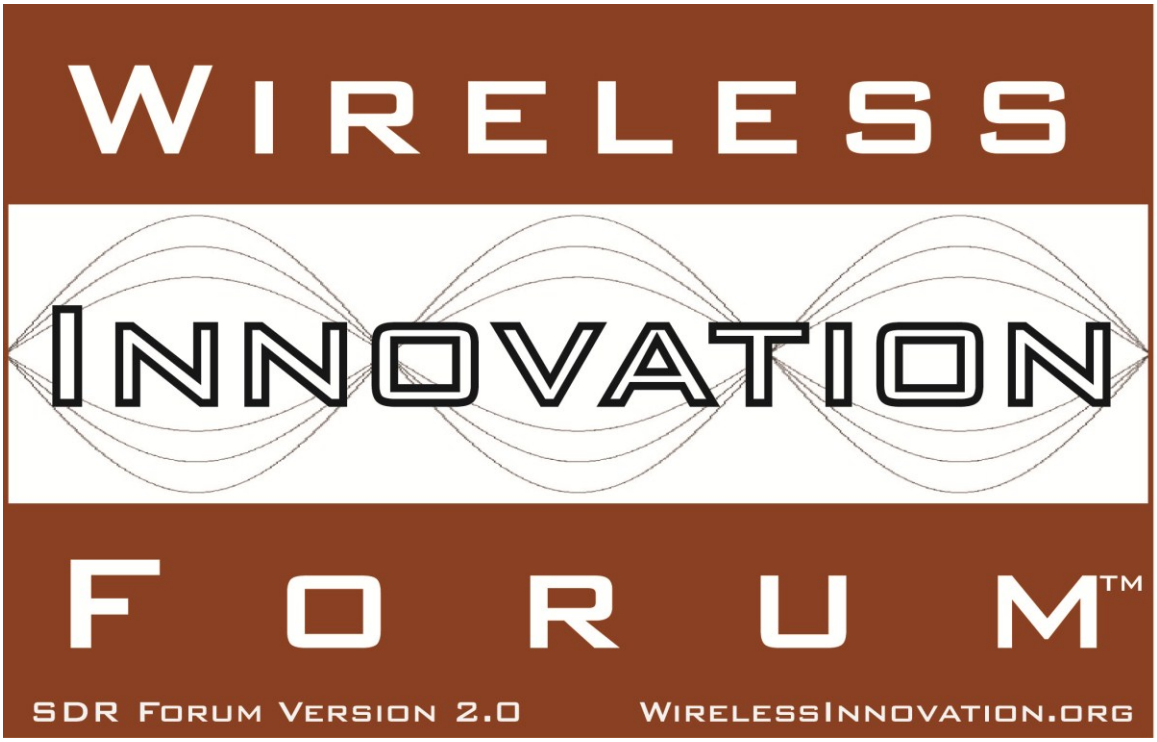

Request for Information (RFI) on Technology for Cognitive Capabilities for Public Safety Communications

Working Document WINNF-10-RFI-0009

Version V1.0.0

16 May 2011

TERMS, CONDITIONS & NOTICES

This document has been prepared by the Public Safety Special Interest Group to assist The Software Defined Radio Forum Inc. doing business as (d/b/a) The Wireless Innovation Forum (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Public Safety Special Interest Group.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

Executive Summary

The purpose of this Request for Information (RFI) is to solicit inputs for an assessment of Cognitive Radio (CR) technology. This assessment is to specifically identify the state of cognitive radio technologies that can provide public safety users with improved functional capabilities, and in particular the capabilities that are identified in two cognitive radio use case documents previously published by the Public Safety Special Interest Group (SIG) of the Wireless Innovation Forum.

The primary output of this technology assessment effort will be a report, generated by the SIG, which will be directed at readers in positions of public safety community leadership, users, researchers, and product developers. The report will help "de-mystify" CR for the leadership and users and provide regulators, policy makers, and standards developers with increased awareness of future technological developments and trends. Researchers and product developers will benefit from the report's identification of technology gaps and dependencies to help define future studies and developments. The report will also be valuable to public safety agencies to help plan communications system life cycles and identify near-term opportunities for enhancement of functional capabilities along with longer-term trends.

These responses will help set a broad research, development and implementation agenda to the community and will be communicated to entities such as the FCC and public safety audiences. Organizations and individuals providing responses to this Request for Information (RFI) will be referenced in the report for their contributions (unless they elect to remain anonymous) and thus can benefit from the enhanced exposure to their potential customers. Furthermore, these responses can help steer the direction taken by potential customers for future systems and technologies.

Contributors

Peter G. Cook	Hypres, Inc.
Fred Frantz	L-3 Communications
Phil Harris	L-3 Communications
Ken Link, Jr.	New Jersey State Police
Stew Potter	Thales
Al Sadowski	North Carolina Highway Patrol
Rick Taylor	Harris Corporation

Request for Information on the Topic of Cognitive Radio Technologies for Public Safety Applications

1 Overview

The Wireless Innovation Forum (www.wirelessinnovation.org) is seeking information on current and proposed Cognitive Radio (CR) technology developments for addressing communications requirements for public safety. We are soliciting inputs from industry, academia, government researchers and users, public safety agencies, and other interested entities. The Forum's Public Safety Special Interest Group (PS SIG), which coordinates the Forum's activities that relate to public safety[1], will use this information for compiling a report that will provide

- education to public safety leadership and users to help "de-mystify" the topic of cognitive radio for the leadership and users;
- increased awareness of future technological developments and trends to regulators, policy makers, and standards developers;
- information for public safety agencies that will to help plan communications system life cycles;
- identification of technology gaps and dependencies to help define future studies and developments for researchers and product developers; and
- a roadmap for technology development to enhance public safety communications capabilities.

These responses will help set a broad research, development and implementation agenda to the community and communicated to entities such as the FCC and public safety audiences. Organizations and individuals providing responses to this Request for Information (RFI) will be referenced in the report for their contributions (unless they elect to remain anonymous) and thus can benefit from the enhanced exposure.

This assessment follows two previous studies[2,3] published by the Public Safety SIG that identifies use cases for cognitive radio technology. Each study included an analysis that documented in detail a scenario describing communications occurring at a major incident; a description of how cognitive communications capabilities could enhance user communications directly relevant to effectiveness of the incident response activities; and a list of desirable cognitive capabilities identified by the SIG.

---

[1] See Appendix 1 for additional information regarding the Wireless Innovation Forum and its Public Safety Special Interest Group.

[2] Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems - Volume 1: Review of the 7 July Bombing of the London Underground, Report No. SDRF-07-P-0019-V1.0.0, available at http://groups.winnforum.org/d/do/1565.

[3] Wireless Innovation Forum, Use Cases for Cognitive Applications in Public Safety Communications Systems Volume 2: Chemical Plant Explosion Scenario, Report No. WINNF-09-P-0015-V1.0.0, available at http://groups.winnforum.org/d/do/2325.

Both studies concluded that Cognitive Radio technology will be instrumental in ensuring that future public safety communication systems will fulfill user needs, but did not discuss the status of technologies that can be leveraged to enable the cognitive capabilities that were identified. Providing this additional technology status information is the purpose for this RFI and the subsequent report that will be developed from the information that is gathered.

Section 2 of this RFI provides a glossary of acronyms used in this report. Instructions for the RFI are provided in Section 3. Section 4 lists the key questions to be addressed in this RFI, and Section 5 provides a conclusion to these questions.

The reader is encouraged to read three appendices that are also provided to help define the context for the RFI questions. Appendix 1 provides additional information regarding the Wireless Innovation Forum and Public Safety Special Interest Group. Appendices 2 and 3 describe "Key Concepts and Issues for Public Safety" and "Related Efforts" respectively.

2 Glossary

The following abbreviations are used in this document:

BER	Bit Error Rate
DSA	Dynamic Spectrum Access
IC	Incident Command
LTE	Long Term Evolution
MHz	Megahertz
MIMO	Multi-Input and Multi-Output
NIMS	National Incident Management System
P25	Project 25
PS SIG	Public Safety Special Interest Group
RF	Radio Frequency
RFI	Request For Information
TETRA	TErrestrial Trunked RAdio

3 Instructions

For inquires about the RFI, please contact the Chair of the Public Safety Special Interest Group, Fred Frantz, at +1 315-339-6184, or via email at fred.frantz@L-3com.com. For inquiries about the Wireless Innovation Forum, please contact Lee Pucker at: Lee.Pucker@WirelessInnovation.org.

We additionally encourage the submission of any relevant white papers or product brochures. The responses to this RFI will be reviewed by members of the SIG, which include industry representatives; therefore do not include proprietary information. The Wireless Innovation Forum intends to use the information it receives in response to this RFI (the "Contributions") to draft reports containing summaries, aggregate data and, in some instances, quotations from the Contributions it has received (with proper attributions of authorship). By submitting your response to this request for information, you acknowledge and agree that Wireless Innovation Forum may, without charge and without further permission, use your Contribution in whole or in

part for the purposes described above, as well as copy, reproduce, distribute and publish part or all of your Contribution, both internally and by incorporating it into future Wireless Innovation Forum publications. Any information that you do not want attributed to your organization should be so indicated.

We are requesting information on cognitive technologies (software and hardware) that can facilitate desired capabilities within public safety radio communications systems. We are specifically interested in learning about existing or evolving technologies and/or products, the technical maturity of the technology, the feasibility of deploying such technologies, and through integration into new or existing products, and information about any non-technical barriers (e.g., regulatory, operational) that may limit or impede deployment.

Within the following section, nine questions are highlighted with a shaded background similar to that for this paragraph, and each question also provides particular areas of interest to help guide the responses, although deviations of responses from the guide are certainly acceptable. Prior to each question, there is a brief narrative to provide background and context for the question. The reader can of course elect not to respond to all questions.

The following information is requested for each answer:

- What technolog(ies) would support the desired capability?
- Describe any product or research project that embodies the technology.
- What is the current state of development for the technology being described (research, in development, prototype, beta test, on market)?
- Are there any regulatory barriers to the adoption of such technology?
- Are there other non-technical (e.g . operational) barriers to the adoption of such technology?
- In what time-frame will the capability be available?

Also, please include contact information that will allow members of the SIG to follow up in the event that clarification of a response is desired.

4 RFI Questions

Cognitive radio technology is rapidly evolving in both military and commercial domains. While certain aspects of today's public safety radio systems incorporate some level of cognitive capabilities (e.g., it can be argued that trunked public safety radio systems and roaming capabilities meet the definition of "cognitive radio"[4]), there is significant potential for much broader application of cognitive radio technology to enhance public safety communications systems. While Dynamic Spectrum Access (DSA) is often identified as the key objective for

[4] The term "cognitive radio" has been defined in a variety of ways. For definitional purposes, we use the definition published in IEEE 1900.1: "a) A type of **radio** in which communication systems are aware of their environment and internal state and can make decisions about their radio operating behavior based on that information and predefined objectives.
b) Cognitive radio [as defined in item a)] that uses **software-defined radio**, **adaptive radio**, and other technologies to adjust automatically its behavior or operations to achieve desired objectives." A more detailed analysis of various definitions of cognitive radio and similar terms can be found in *Cognitive Radio Definitions and Nomenclature,* Document SDRF-06-P-0009-v1.0.0.

cognitive radios, there are additional potential applications of cognitive radio technology that the Public Safety SIG identified in the two detailed studies referenced in Section 1. The questions that follow pertain to these applications.

4.1 Interoperability for Public Safety

A number of technological and operational issues remain for voice and data systems that often impede the emergency responders' ability to interoperate because of incompatible systems. Current technological solutions for providing voice interoperability through disparate systems run the gamut from console patches to cross-band repeaters to audio switches to network-based solutions. Current implementations facilitate interoperability, but they typically require a layer of additional equipment external to the core communications systems. Bridge devices typically require the same transmission to be concurrently broadcast over multiple radio systems and frequencies within the same geographic area, thereby requiring additional system capacity and spectrum. Deployable repeaters and switches often require time to mobilize, and once on-site require additional time to configure and activate.

Question 1:

Contrary to the external devices described above, please provide information on innovations that are native to end user radio equipment and systems, minimizing or eliminating dependence upon an overlay of specialized interoperability equipment, patched transmissions, and so on. Examples of such innovations include, but are not limited to, the following:

a) "Smarter" gateway devices
b) Advanced interoperability concepts utilizing multiband radios
c) Innovations for interoperating between P25 and other standards (e.g., TETRA)
d) Innovations for enhanced data interoperability (e.g., interoperability among disparate mix of broadband through low speed data systems)
e) Interoperability between new and legacy capabilities (e.g., voice interoperability with broadband network
f) Innovations that standardize procedures to facilitate the ability of "visiting" responders to appropriately access communications systems (such as a "meeting point")
g) Creation of a "Virtual System" from multiple disparate system

As with interoperability between public safety agencies, the SIG Use Case documents (referenced in Section 1) identify a significant requirement for interoperability between first responders and non-public safety communications systems. For example, communications may be required between first responders, emergency management, and other organizations such as other civilian government authorities (e.g., public health, public works, transportations), organizations supporting critical infrastructure (e.g., utilities), tow truck and bus drivers, National Guard, Department of Defense units. In some cases it also may be beneficial to allow more seamless communications capabilities between selected cell phones and the public safety network, of course with appropriate restrictions. This need can arise during major disasters and events as well as daily challenges faced by public safety agencies.

Question 2:

Please provide information regarding innovations that will enhance communication between non-public safety resources and public safety users. Examples of such innovations include, but are not limited to, prioritization of access and throughput, store-and-forward capabilities, integration in support of incident command (IC) structure operations, and maintaining the security and integrity of public safety communications.

4.2 Coverage Improvement

System coverage, i.e. providing radio access to voice and data system resources, is an important requirement in a public safety communications system. The ideal solution for a public safety communications system would provide access to all services at 100% of the locations where a first responder may be needed, 100% of the time, with perfectly understandable voice quality and/or ensured data delivery at acceptable data rates. This would include 100% access within traditionally difficult locations such as basements, stairwells, tunnels, and buildings where users often experience well over 30 dB RF signal penetration loss. Cost-benefit tradeoffs made when procuring and designing public safety communications systems (as well as immutable factors such as the laws of physics), result in systems that do not meet the ideal solution of ubiquitous access. Also, in recent real-world cases like the London Bombing and Katrina disasters, system access was further (and severely) compromised by loss of key supporting infrastructure, such as radio network base stations, radio towers, and tunnel coverage devices. Thus there is a continuing need to develop cost-effective means for improving system coverage in general, as well as provide capabilities to rapidly adjust to the loss of infrastructure that impacts coverage.

Question 3:

Please provide information regarding solutions for enhancing public safety coverage. Examples of such solutions may include, but are not limited to, the following:

a) Reconfiguration of responders' radios, creating an ad-hoc extension to an existing network. Such network extension would allow transmissions to be passed back and forth from the incident site through a network of individual responder radios operating in peer-to-peer mode effectively extending coverage of the main radio system/network.
b) Use of adaptive beamforming antennas to maximize gain in the direction of the desired communication path and/or minimize gain (create a null) in the direction of a known interfering signal.
c) Standards for interfacing "smart antennas" with cognitive radios (to define parameters such as band, power capability, direction, null direction, polarization, and so on).
d) Adaptive modulation and/or data rate adjustment for modifying the link budget and interference generation (on transmit) or suppression (on receive)
e) "Smart" frequency control to increase frequency separation between interference sources and the desired radio signal. Adaptively change/modify receiver filter characteristics to provide improved rejection of an interfering adjacent signal (e.g., by narrowing the receiver filter bandwidth) or improved sensitivity when interference isn't limiting coverage
f) Enhanced roaming algorithms

g) Enhanced and/or adaptive channel coding algorithms
h) MIMO techniques
i) Adaptive receive processors

As another means for enhancing coverage, access to non-traditional network resources may be a viable option for public safety. For example, additional data bandwidth may be operationally required even in areas where voice coverage and capacity meet user requirements. Broadband services provided via TV spectrum whitespace, or access to commercial services via cellular provider data facilities may be exploited as a supplemental, or fallback, resources. For example, commercial coverage might be available in a tunnel where specific public safety systems are not. Access to supplemental resources would require appropriate wireless communications equipment in vehicles, and appropriate policies must be formulated and implemented, defining when such links could be activated.

Question 4:

Please provide information regarding non-traditional network solutions for coverage enhancements and/or backup public safety use, including provisions for priority that can be made available to public safety users and necessary changes to existing systems that would be necessary for the solutions.

4.3 Spectrum Utilization Optimization and Dynamic Spectrum Access

One of the critical issues faced by the public safety community is limited availability of RF spectrum to address current and emerging requirements for mission-critical communications. Increasing public safety reliance on bandwidth-intensive data such as video, paired with continuing reliance upon a limited number of narrowband voice channels when responding to large scale complex incidents, creates increasing pressure for spectrum resources. Cognitive radio technology shows promise as a technological path for addressing this issue.

Question 5:

Please provide information about technologies that can provide the following capabilites:

a) Identify and optimize network capacity and loading. For example,

- prioritization of transmissions.
- control of access priority, per subscriber unit.
- adjust network operations to accommodate significant changes in traffic volume.
- accommodate direct communication between first responders and non-first responders.
- re-allocate spectrum used by public safety users as incident response communications demands decline.
- Identify and mitigate capacity issues with wireless or wireline backhaul components of the network.

b) Dynamically access additional spectrum resources in the most effective manner, consistent with regulations and policy. For example,

- identify situations, and associated threshold criteria, whereby dynamic spectrum access can be initiated.
- identify available spectrum resources that can be utilized (sensing and policy limited).
- exploit all available spectrum resources as needed, and integrate additional spectrum resources into existing communications capabilities, including disparate frequency bands and protocols.
- adjust spectrum utilization based on defined regulations and policy [e.g., a network sharing agreement].
- aggregation of multiple radio networks to provide improved data rate, coverage and redundancy.

4.4 Communicate Reconfiguration Information

Public safety communications are generally provided through a network consisting of some infrastructure and accessed through number of end-user (subscriber) devices. Thus system reconfiguration decisions cannot occur independently, and must be coordinated through all network components. Decisions must be based on knowledge of the current configuration of all nodes that are part of the network, and reconfiguration commands must be transmitted to affected nodes securely and reliably.

Most public safety network configurations are static, based on a pre-planned configuration. Some networks have a limited ability to communicate reconfiguration information, such as an ability to distribute encryption keys and re-key end user devices over-the-air.

Question 6:

Please provide information about technologies that can provide the following:

a) Query/exchange information among the network infrastructure and end user radios. Examples of information include, but are not limited to vendor, network/end user radio type, and capabilities [e.g., available modes, version numbers, reconfiguration capability, etc.] Also, suggestions for standard methods for transmission of network information are solicited
b) Identify and communicate accessible spectrum resources that can be utilized to offload some calls based on real-time identification of available spectrum.
c) Reconfigure [subscriber and/or network radios and antennas] to access additional spectrum resources when required
d) Rapidly adjust air interface transmit power, waveforms, frequencies, filtering, and receiver attenuation (based on network & end user radio commands).
e) Specify and reconfigure as appropriate air interface transmit and receive parameters, on a transmission or message sequence basis.
f) Reconfigure/Reprogram radios over the air with ensured integrity

4.5 Manage Communications Resources

Real-time management of network resources is critical, particularly when specific situations in which incident communications requirements exceed system capacity, creating a need for more effective network resource management tools than those that are commonly available today. The

likelihood of the occurrence of such situations will increase as bandwidth-intensive applications such as video become more prevalent in incident response. Optimizing public safety spectrum use in critical situations and ensuring that available spectrum resources are accessed in support of the most critical operational needs (regardless of how specific spectrum resources are allocated) on a real-time basis, will be critical for ensuring that effective in communication capabilities are maintained for future incident, responders. The required innovations are critical regardless of whether applied to public safety-only networks or shared public-private networks.

Question 7:

Please provide information about technologies that can manage communications resources. Examples of possible related innovations include but are not limited to the following:

a) Monitor network resource allocation & associated issues, including, but not limited to anticipating network resource allocation issues and providing an effective display of current conditions and generate appropriate alarms.
b) Provide information about the RF environment at a user's location.
c) Geolocate network nodes
d) Predict signal and interference levels at any potential subscriber location.
e) Communicate in a standardized way information about that status of communications assets to support network utilization and Comm Unit Leader[5] functions and tools

4.6 Support Incident Command

Typical public safety mutual assistance activities involve personnel responding from multiple agencies and arriving on scene as part of large incident response. Given the scope of large incidents, responders may be from jurisdictions for which there are no standing mutual aid agreements and in place and not equipped to support pre-planned communications interoperability capabilities. This means that upon arrival to the incident their radios may not be directly interoperable with local communications systems being used to manage incident response. A desired technological capability is that radios arriving with visiting first responders can be dynamically reconfigured specifically to support the in-operation pre-defined incident response, and also specifically support the arriving responders' role within the incident response structure.

The capability that an arriving radio should provide is defined by a function of the role that the responder user is performing—for example, supervisors in the incident command structure require specific capabilities that responders in other roles do not. This concept provides the incident response management team greater control of communications resources, ensuring that ubiquitous interoperability does not result in "everyone talking to everyone at once on the same frequency." After arrival on scene, following radio reconfiguration to support a responders' role, mechanisms must also be in place to ensure that a device reconfiguration was successfully executed.

[5] Comm Unit Leader is a specific function defined in the National Incident Management System (NIMS) adopted as a standard in the United States for incident response. Other incident management systems/procedures are assumed to have comparable functions.

In today's public safety environment, unlike devices in commercial cellular networks, reconfigurations are typically manual in nature completed and require a responder to report to an incident staging area equipped to make radio modifications. In addition, radio configuration templates are based on static definition of communications capabilities, independent of the actual role that the responder has in supporting the incident command structure.

Question 8:

Please provide information about technologies that can support incident command. Examples of possible related innovations include but are not limited to the following:

a) Identify an over-the-air "meeting point" for incoming responders to register and receive configuration information
b) Associate users, radios, radio capabilities, and user roles [e.g., roles within a NIMS construct]. For example,
- Define explicitly [i.e., in a machine-interpretable form] user roles within an incident response structure.
- Store in a machine-interpretable form a user's credentials.
- Authenticate a specific user as qualified for a specific role.
- Define appropriate radio capabilities in support of a specific user's role.

c) Dynamically reconfigure communications capabilities (both subscriber and network capabilities) using criteria based on both the user's current role, and incident policy, mitigating how dynamic reconfiguration negatively impacts ongoing communications and minimize bandwidth required to support over the air transmittal of device reconfiguration information

4.7 Rollback Configuration Changes

Given the capability to reconfigure communications capabilities in near-real-time, there must also be a capability to undue, or roll back, changes if they result in unintended consequences, otherwise degrade communications, or to simply restore a communications device to a pre-incident configuration. For the situation in which a reconfiguration needs to be rolled back, networks and subscriber devices may maintain a configuration history that allows previous configurations to be restored. However, rolling back a configuration change that involves the network and subscriber equipment is not typically automated in current systems. Thus changes that turn out to have a negative impact on communication usually can only be reversed by manually resetting subscriber equipment software configurations.

In the case of restoring default or home agency configurations as a responder is released from an incident, the most significant shortfall is associated with radios that cannot be reconfigured over the air. Reprogramming radios that must be tethered to programming hardware can currently take a significant amount of time (days or weeks) due to the logistics of transporting radios to a reprogramming point and manually loading configuration software updates. Radio security is not specifically addressed here, but some LMR manufacturers require use of special hardware or software keys prior to accessing radio configuration functions, creating additional logistical challenges.

Question 9:

Please provide information about cognitive radio technology that can support rolling back cognitive system configuration. Example capabilities include, but are not limited to:

- Storing [previous] device configuration information.
- Recognizing when a device reconfiguration results in a degraded capability.
- Restoring [or rolling back] the device capabilities to a previous configuration.
- Rapidly restoring a default configuration and/or the configuration of the device prior to the incident.

5 Conclusions

The questions and comments above are intended to elicit information on new approaches to solve problems encountered by the need of Public Safety first responders to communicate. As many of these difficulties have been experienced in the context of currently operational technologies, they may reflect paradigms or perspectives inherent in more mature functionality. The Forum does not wish to impose any specific context on responses to their RFI. Responders are encouraged to "think outside the box", and not be limited by existing constraints. Introduction of new architectures and concepts clearly involves transitions that must recognize and overcome such conditions, but we do not want to impose them in a way that will inhibit creative thinking.

Appendix 1 Additional Information on the Wireless Innovation Forum and Public Safety Special Interest Group

The Wireless Innovation Forum™ is a non-profit "mutual benefit corporation" dedicated driving technology innovation in commercial, civil, and defense communications around the world. Forum members bring a broad base of experience in Software Defined Radio (SDR), Cognitive Radio(CR) and Dynamic Spectrum Access (DSA) technologies in diverse markets and at all levels of the wireless value chain to address emerging wireless communications requirements through enhanced value, reduced total life cost of ownership, and accelerated deployment of standardized families of products, technologies, and services. The PS SIG is an organization within the Wireless Innovation Forum that provides a focus for activities in which the public safety community has an interest. Goals of the PS SIG are to interface with both communications users and commercial vendors associated with the public safety community with a goal of increasing awareness of SDR related issues, publicize activities of the Forum that address those issues, and increase participation by the public safety community in Forum activities. The PS SIG also interacts with other forum committees and working groups to ensure that the public safety community's inputs are addressed in other publications and initiatives undertaken by the Forum.

The public safety community, as defined by the PS SIG, includes all first responders (e.g., emergency medical services, fire services, police/law enforcement. It also includes secondary responders (e.g., civil government, emergency management, environment health personnel, civil protection/homeland security/homeland defense units, search and rescue units, hospitals, relief organizations, public utilities, transportation), and other elements of the criminal justice system.

Appendix 2 Key Concepts/Issues for Public Safety Communications

One of the most important fundamental requirements associated with public safety communication needs is the ability for first responders to communicate as needed, regardless of technological differences in communications equipment (e.g., different frequency bands, different protocols, different modes, manufacturer specific capabilities, different versions of hardware and software). Most of the effort in recent years has been focused on enabling "mission-critical" voice communications. There are still open challenges related to achieving ubiquitous voice interoperability, although concerted efforts in development of technology, governance, standards, have led to vast improvements. Gateway devices and multiprotocol land mobile radios are common and multiband radios are beginning to penetrate the market. However, even today many current interoperability approaches do not utilize spectrum in the most efficient manner.

As significant progress is being made to address the challenges associated with interoperability, public Technological advances that drive commercial thirst for spectrum also provide the foundation for public safety applications that also require increasing access to spectrum. These applications provide a wealth of information to public safety users such as the ability to download security video to a police car, devices that monitor firefighter biometrics and equipment safety and are turning attention to other equally challenging issues. Spectrum availability is an issue for all wireless systems, including those for the public safety community in that spectrum resources currently allocated to public safety users are limited. Mission critical information such as status and real-time access to hazardous material information is resulting in increasing data transfer through wired and wireless networks in addition to voice traffic. The resulting information volume has the potential to overwhelm communication network resources and capabilities as well as the ability of responders to process information.

In response to the continuing growth in data volume, U.S. public safety user groups have endorsed LTE as the protocol of choice for 700 MHz broadband data (as a national option) and the FCC has identified this technology as a requirement for use in 700Mz public safety broadband spectrum.

An increasing reliance on resources and capabilities enabled through wireless broadband data technology has created new interoperability challenges associated with:

- multiple networks and wireless data networking technologies;
- multiple frequency bands;
- multiple protocols and varying protocol implementations;
- constantly evolving wireless technology standards
- multiple encryption approaches
- increased complexity of data
- migration of voice services onto data networks.

Current proposals for a national broadband network in the 700 MHz frequency band present a significant opportunity for public safety to have a dedicated network built from the ground up following standard protocols. However, we strongly believe that there is a significant role for evolving cognitive radio technology. Spectrum efficiency will continue to be a critical aspect of a nationwide network. Efficient management of resources will be critical, as will exploitation of additional spectrum when requirements surpass existing resources (e.g., leveraging 700MHz, 4.9 GHz, unlicensed, and white space spectrum in a major emergency). Other issues will include graceful upgrade of product software, graceful migration to evolving technologies, logistics associated with provisioning and support, leveraging commercial hardware and software development, improved efforts while addressing unique public safety needs, maintaining ease of use, and reducing life cycle costs. Maintaining robust and reliable communications in the face of intentional or ambient interference will continue to be an issue. Costs, extended lifecycle timeframes and affordability have traditionally been limiting factors limiting the extent to which the public safety community has been able to refresh and deploy new technologies.

Future public safety communications platforms will likely be implemented as a system of systems reliant upon on a variety of networks. They will involve emerging network technologies, standards, protocols, and frequency bands, and differing implementation choices made by network operators in support of local user needs. These networks must support services ranging from short-range communication capabilities such as those provided by personal area networks, to long haul communication at a national or international level. We believe software defined and cognitive radio technologies can provide capabilities that exploit all available communications resources to facilitate interoperability and support seamless “virtual” communications capabilities to public safety users.

Appendix 3 Related Efforts

The there are several, concurrent, ongoing commercial and government efforts focused on addressing the needs of public safety personnel and agencies. This RFI effort, undertaken by the Public Safety Special Interest Group, is intended to build upon, and complement, these efforts.

The following list is not exhaustive, and focuses on government initiatives that also address the overall issue of leveraging evolving technology for public safety. (Technology research activities are not included in this list, but rather are the types of information that we are soliciting through this RFI.)

The National Institute of Justice (NIJ): NIJ conducts research and development on technologies for state, local, and tribal law enforcement and criminal justice needs. NIJ's communications portfolio includes research, development, test, and evaluation activities that include development of cognitive radio technologies developed in response to identified public safety needs. NIJ is currently funding research into a number of software defined and cognitive radio topics, such as:

- Automated discovery of public safety networks
- Reconfigurable radios
- Intelligent, handheld land mobile radio network bridging
- Steerable directional antennas
- Smart power management
- Network switching to avoid disruption
- Channel/path bonding

The Department of Commerce: The Department of Commerce Public Safety Communications Research (PSCR) program acts as an objective technical advisor and laboratory to DHS/OIC and the response community to accelerate the adoption and implementation of only the most critical public safety communication standards and technologies. PSCR examines public Safety Requirements, Specifications/Standards, Test and Evaluation, and records Lessons Learned. PSCR support includes technology research in support of the following:

- Radio over Wireless Broadband,
- Project 25 support (i.e., P25 compliance assessment, P25 standards development, P25 Security, P25 ISSI),
- Public Safety Voice over IP and
- Research in support of public safety Audio and video quality.

The Public Safety Communications Research (PSCR) program is deeply involved in the rapidly progressing topic of Public Safety 700 MHz Broadband (e.g., Public Safety LTE test and demonstration network as well as LTE PS standards support). To help move forward broadband technology for public safety communications, PSCR is building a national public safety broadband demonstration network and providing technical advocacy for the public

safety community through requirements gathering and standards development. More details can be found at www.PSCR.gov.

The Department of Homeland Security (DHS) SAFECOM is a public safety-driven communications program, managed by the Office of Emergency Communications and the Office for Interoperability and Compatibility (OIC) of the U.S. Department of Homeland Security. SAFECOM works to build partnerships between all levels of government, linking the strategic planning and implementation needs of the emergency response community with Federal, State, local, and tribal governments to improve emergency response through more effective and efficient interoperable wireless communications. Under the SAFECOM program, public safety communications Statement of Requirements and Architecture Framework documents have been published. More details can be found at http://www.safecomprogram.gov/SAFECOM/.

The National science Foundation (NSF) is sponsoring a research & development program entitled Enhancing Access to the Radio Spectrum (EARS). The EARS program "… targets innovative and potentially transformational research that carefully considers the interplay of science, engineering, technology, applications, economics, social sciences, and public policy on spectrum efficiency and access."[6]

The European Telecommunications Standards Institute (ETSI)): The ETSI Technical Committee on Reconfigurable Radio Systems (RRS) has a Working Group specifically focusing on the application of software defined radio and cognitive radio technology to public safety.

The Federal Communications Commission (FCC) is addressing regulatory aspects of DSA technology (including proceedings that are asking specific questions regarding the regulatory considerations of deploying DSA in public safety communications.

This RFI effort undertaken by the Public Safety Special Interest Group is intended to build upon, and complement, these efforts.

[6] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503480, accessed 28 February 2011.