Before the
Department of Commerce
National Institute of Standards and Technology
Boulder, Colorado 80305

In the Matter of:	)	
	)	
Soliciting Input on Research and Development	)	
Priorities for Desirable Features of a Nationwide	)	Docket No. 110727437-1433-01
Public Safety Broadband Network	)	
	)	
	)	

COMMENTS OF L.R. KIMBALL

L.R. Kimball, a CDI Company, of Ebensburg, Pennsylvania hereby submits comments in response to the *Notice and request for comment* released by the Institute on September 6, 2011, in the above captioned proceeding.

L.R. Kimball is one of the nation's largest engineering/architecture/consulting firms, annually ranked among the top 200 design firms and the top 20 telecommunications firms by Engineering News Record. L.R. Kimball's Communications Technology Division has offered public safety and mission critical consulting services for more than 15 years. Our telecommunications and technology practice is focused on all facets of public safety, supporting operations and technologies; 911 networking, call delivery and call handling; radio communications; cyber security; and public policy.

COMMENTS

L.R. Kimball responds to the following items regarding the features identified in the *Notice and request for comment* with the chart below.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

- Current gaps that exist preventing the realization of the full potential of the feature;
- Possible research and development that could take place to close any technical gaps;

Feature	Importance	Notes/Gaps/Challenges
Features to ensure resiliency in an emergency		
Resiliency	High	The ability to recover from issues is important to a public safety system. It is better to AUTOMATICALY recover. Components should have a minimum of n+1 resiliency.
Self-Organizing	High	The ability of the network to self-organize and reroute based on the current situation within the network is important and is one of the major benefits of an IP infrastructure over the current systems.
Meshing (Data)	Low	Mesh operation in a data mode has some benefits, in particular at incident scenes to enhance the abilities of low powered systems, or to maintain the ability to transmit data in off-network areas but this has a major drawback on bandwidth and potential interference if used extensively. This is one area of potential R&D. The objectives would be to determine specific limits on hops, and automatic methods to avoid interference with multiple systems.
Meshing (Voice)	High	The potential to provide localized and unit to unit voice communications even when off-network based on Mesh capabilities deserves further research and development. The viability of this mode for off-network voice requires further investigation to determine if it can support the mission critical performance public safety responders require, and if the low power subscribers operating in a mesh environment for voice can achieve reliable coverage in and around buildings.
Adaptability	High	The ability of the network to adjust to the situation, or to be told to adjust, is important for public safety. This should be an automatic process. Decisions for most situations in policy based systems should be developed and decided before the situations arise.
To ensure reliability and availability		
Prioritization	High	Prioritization is important, but how to prioritize is an issue. In traditional networks today, certain types of packets are prioritized such as voice. There needs to be further prioritization on a public safety system based on service type, user, or even a specific message. This is an area of R&D to determine how this can be accomplished without impacting interoperability.
Quality of Service (QoS)	High	See comments on prioritization.
To enable security		

Feature	Importance	Notes/Gaps/Challenges
Strong, Dynamic Access Control	High	It is critical to protect the information of a public safety system. One area of R&D could be to share that information between different systems: how does one state recognize users from another state, or when roaming between systems. Another R&D issue would be to look at public records issues. This is usually a state issue, does there need to be federal input on the use of these networks?
To ensure affordability/commercial alignment		
Compatibility with Commercial Infrastructure	High	This will benefit the system because equipment costs will be lower due to the ability to use existing commercial research and development and then build on it. This will also add to the security issues of the system. Using commercial infrastructure opens up the ability for unauthorized access from outside entities. The commercial infrastructure is not controlled by public safety and security actions will be needed. The QoS on commercial infrastructure will also need to be implemented. In one project where IPSEC tunneling was used through the commercial internet, Voice communication was negatively impacted each afternoon due to possible bandwidth sharing.
Network sharing	Medium	The context of the notice identifies this as sharing with public carriers, which will be good for areas that do not have public safety service. However, the issue of sharing will involve federal, state, and local policy issues. A good example of the sharing and prioritization need is in the SAFECOM Statement of Requirements for Communications and Interoperability. This document discusses the need to choke or even shut off certain users and or services in certain situations. Using a public network will prevent the ability to choke or shut off services. An example of this is the current Telecommunication Service Priority (TSP). While TSP is a good service, there is a built in delay of communications for users as they get access when available. This would adversely impact a public safety system for primary communications.

Feature	Importance	Notes/Gaps/Challenges
Multi-Modal	High	This is in keeping with the expectations of the public and will provide more capabilities for the responders. The impact of video is just beginning to be felt by public safety, but any system must support it. The ability of the network to ultimately support public safety voice in the same manner as traditional LMR (PTT one-to-many, on and off-network, etc.) seems to be an expectation and requirement. Providing this capability in a multi-modal environment could be even more challenging and therefore is an element that definitely requires focus by NIST.
Scalability	High	Any system will need to be scalable and automatically scalable on the fly. Incidents are rarely scheduled. If you need to contact a provider to scale the system while responding to a situation it will not be a viable solution.
Power Awareness	Medium	This is a good feature for use of equipment with batteries. Users will need to carry devices and use them for normal shifts of 8 to 12 hours and incidents that may last even longer. In many current commercial systems, the power is controlled by the network and it tells the device what to do. This has lead to issues with some functions of the user device being powered down when it needs full power to perform a critical function like location acquisition in a network based location determining system.
Standardized Common Interfaces	High	This is critical, but further defining which standardized interfaces will be important, and the details for each. For example a standard is usually written for a larger stakeholder group, the Public Safety systems will most likely need to define the specific components of these standards to ensure interoperability. Avoiding proprietary solutions that will require licensing and choice of vendors is important. This may also lead to faster innovation as multiple vendors will work on improving services rather than relying on a single entity.
Uniform, Universal Access	Medium	A wide choice of access will help to gain acceptance, but opens issues of security. Defining a large set of access devices and methods may better benefit public safety.

- NIST requested comment on the importance of employing open standards for the nationwide public safety network?

L.R. Kimball responds that it is clear that the establishment and adoption of open standards for the nationwide public safety broadband network will be critical to its success. The promise of this network to not only provide the bandwidth needed to transport data and information never before available to responders, but to also ultimately provide true interoperable voice communications will only be met if the network and all elements are built on open standards.

Over and above the relatively obvious need for standards to assure interoperability across the network and between devices for Public Safety, there are some specific considerations that must be addressed in establishing LTE related standards for Public Safety. First, as a "commercial" technology, defining and establishing consensus standards from the carrier and manufacturer industry are well underway and already defined and roadmapped by the 3GPP.

In order to take advantage of the economies of scale from leveraging commercial LTE development that will help keep down costs for both infrastructure and UE, Public Safety must participate as well in that standards process. In addition, Public Safety must develop a full understanding of the elements and roadmap defined by 3GPP, in order to identify the gaps between the commercial LTE standards, and the features and specifics needed by Public Safety. Once these gaps and difference in need are fully understood, Public Safety can pursue development of a standards "layer" building upon and taking advantage of the commercial standards. We recognize efforts and activity is already underway to define the understanding of Public Safety voice and data needs on the LTE platform (i.e. the Statement of Requirements, findings from the NIST PSCR broadband demonstration project, etc.) L.R. Kimball wishes to emphasize the importance of developing the means to address these needs and features by building upon the LTE commercial standards foundation to every extent possible.

For the most part, in today's Public Safety LMR environment, referring to "standards" tends to particularly mean the air interface or standard – such as the P25 CAI. Even though the P25 standards suite is to include establishing interface standards that would potentially allow buying one manufacturer's console to interface to another's trunked system, or the use of one manufactures' base stations in another's network, this scenario has not yet quite materialized.

In order to continue down the path currently underway for Public Safety broadband - locally/regionally procuring and build-out of elements that will become a single, integrated nationwide network – standards and interfaces must be in place and followed at all of the building block levels including eNodeB and RAN, EPC, gateways and supporting system access and management applications, and of course UE. Again, building from the standards established from the 3GPP, Public Safety, through the R&D efforts of NIST, we must establish any additional detailed standards requirements specific to our needs so that manufacturers can address these standards and systems being procured and can build them using equipment that will allow different manufactures equipment to operate within and across the overall integrated national network.

- NIST requested comment on what challenges public safety could face in realizing the full potential of these features given currently implemented solutions, and what network features or requirements have not been identified above, the lack of which may impair the network's ability to adequately serve the needs of public safety.

L.R. Kimball responds that Public safety could face challenges realizing the full potential of the broadband network given currently implemented solutions;

Most issues and roadblocks to development and adoption of the national Public Safety Broadband network will go back to the following two challenges:

- Funding
- Control

Although the issues of control and funding might appear to be outside the scope of NIST's request for inputs related to development of features for Public Safety, we believe some important technical work and development is needed to address the control aspect of these networks.

Traditionally, most agencies and jurisdictions have built and owned their public safety radio systems. Even with modern trunked platforms technically capable of scalability and supporting large numbers of sites and subscribers from a single switch, it remains difficult to overcome control concerns and encourage sharing of a common switch. In order to be successful, and take advantage of the scalability and capacity supported by LTE networks, these systems will need to be developed and managed by an accepted entity, such as was done with NLETS. The development of an effective governance structure and a trusted authority will be key to widespread adoption.

Regardless of the ultimate governance body and structure that would oversee the construction of these networks, appropriate tools and applications will be required to manage resources, system access, priorities and provisioning. Conducting the R&D needed to define the requirements of these system management application tools, and then fostering their development is an an area that NIST could and should include as a high priority element of their efforts.

The applications and system management tools that exist today for commercial technologies such as LTE have primarily been developed to allow carriers to manage and track subscriber usage, air-time, etc. for billing purposes, activations, etc. as well as general "system management." These applications and specific approach to system management and provisioning are likely customized by each carrier to reflect their business operations and approach to system management.

When we consider the environment of a national, Public Safety broadband network, serving hundreds or thousands of local and state agencies and jurisdictions, providing the tools

and applications that present some measure of control and management will be a significant factor in the speed of adoption by these entities.

The availability of system/subscriber management and monitoring tools and applications, providing an appropriate level of access and control for local agencies and jurisdictions could not only be a critical factor in the adoption rate as the network is constructed, it could also impact the early stage consensus on the approach to architecting the network. NPSTC, NIST and many others have recommended the assignment of a single PLMN for the network and related discussions center on the potential to cost-effectively architect it with a small number of EPC's. At the same time, many jurisdictions are already involved in discussions with vendors, pursuing RFP's or actually contracting for local or regional LTE systems.

There are a number of valid reasons these entities are moving forward with LTE system procurements, and this is not meant to criticize this activity. However, we believe this localized approach to procuring these systems illustrates the difficulty that will be encountered in moving from a mindset of locally owned and controlled radio systems to one which is owned, operated and governed by others. The availability of system management and monitoring applications at a local jurisdiction level won't address all the aspects involved in changing this traditional mindset, but could certainly help overcome some of the potential concerns.

With this background in mind, some of the R & D elements that might be explored by NIST related to system management and monitoring – both at the network level and at the local or jurisdictional level include:

- What features and functionality in the broadband network require some level of access or control at a local or jurisdictional level?

    - Examples – prioritization of traffic, subscriber provisioning and activations, usage levels and reports, roaming capabilities, etc.
    - What functions or operations could be managed at a network operator level vs. features that might require rapid access and changes at a local level in order to respond to an event?
- What capabilities and system management tools have already been developed and are used by carriers for the various levels of management and provisioning of commercial networks?
    - Can these applications or elements of them be leveraged to develop the tools needed to address specific public safety system management and monitoring needs – both at an operator level and local level?
- Are there any potential new hardware or software development efforts needed on the system RAN and/or UE to support unique Public Safety system management function or feature requirements?
    - Are there elements or interfaces here that require further definition as part of standards in order to assure any vendors equipment is compatible with the system management and monitoring tools developed for public safety jurisdictions?
- Presuming that support for voice on LTE continues to be developed and evolve on the Public Safety Broadband network, what capabilities for managing voice and related features must be supported by the system management application?
- Can system management and monitoring tools be developed that allow partitioning of users/jurisdictions to access only their users and resources?
- How can local access be provided but network security and protection be maintained?

- What interaction, if any, might be required between these system management and monitoring applications and the user applications on the network?
    - For example, routing video to multiple locations/devices, bandwidth allocation and QoS, etc.
- What interaction or support might be needed from these system management applications relative to interface and interoperability with legacy LMR systems such as P25 trunked voice?
- Given the likelihood that Public Safety UE will be roaming on commercial networks, would the system management applications for the public safety broadband network need to interface or pass information to/from the commercial LTE networks?

It is our observation that NIST is in a unique position to address and drive the definition and development of the various elements and requirements of Public Safety broadband identified in the *Notice and Request for comment* and elements such as system management and access. With the LTE system elements already in place under the PSCR project, and the funding for further R&D under the proposed legislation, NIST can drive needed neutral oversight and coordination for defining and developing the extensive functions and features specific to public safety broadband.

In addition to the list of specific elements NIST identified in the request for Comment and other recommendations for further R&D efforts such as system management and monitoring tools, L.R. Kimball suggests that some focus be applied to assuring there is full alignment between the potential applications and information needed by public safety, and the capabilities

of the network to support these. Certainly, one the most referenced applications for public safety broadband is “video.”

Access to/from video at a scene will clearly provide substantially increased situanal awareness for responders, dispatchers and administrators, it’s our opinion that more research is needed to fully explore the use-cases, and an understanding of just how it will be used, what are the realistic bandwidth requirements of different use cases, etc. Having a better understanding of the uses in public safety responses of a potentially high bandwidth application such as video could impact some of the technology development requirements for LTE that NIST is seeking to address.

Other applications – and technology advances underway in Public Safety should also be considered and understood before finalizing the requirements of public safety broadband and developing the capabilities unique to public safety. One of these areas for further research is the interface, and potential interaction with NG 9-1-1 networks. The potential synergy of the “inbound” information side of the dispatch process to the “outbound” responder side of the equation may not be fully understood or appreciated until these networks begin to be deployed and used. However, R&D efforts should be made now to examine and understand any potential requirements for interfaces or services that should be developed in the public safety LTE platform to assure that full advantage could be taken for the efficient and full flow of information (video, stills, data, etc.) that NG9-1-1 networks will enable.

- NIST requested comment on how NIST should pursue the recommendation from a recent report of the President's Council of Advisors on Science and Technology that suggested the need to develop methods for implementing a ``survivable core'' of cyber-infrastructure that would be relied upon to provide truly essential services in the event of a catastrophic cyber-attack. Please comment on. Among other things, commenters should address whether the goal should be to design a separate survivable core that is integrated

> and interoperable with the primary public safety network, or instead to design the primary network such that it can reconstitute rapidly--following a catastrophic event--to achieve some ``core'' level of service.

L.R. Kimball responds that the public safety industry is currently undergoing a radical evolution. The introduction of NG9-1-1 brings necessary and exciting changes to the nation's public safety system. The benefits of these changes will allow public safety agencies to address the increasingly complex and advanced technologies that our society uses on a daily basis and will significantly enhance their ability to continue the important task of savings lives. However, while the benefits of NG9-1-1 are both obvious and substantial, the risk of Cyber Security attacks on the nation's public safety infrastructure is increased with the evolution towards NG9-1-1. This stems primarily from the simple fact that 9-1-1 call centers will become interconnected through the use of IP-Enabled Emergency Services Networks (ESINets), some of which may include broadband wireless segments or portions. These networks, while necessary to fully realize the benefits of NG9-1-1, dramatically increase the need to ensure that comprehensive and holistic cyber security countermeasures are implemented in a consistent and meaningful manner—something not historically done within the public safety industry. A survivable core of cyber infrastructure that could be relied upon to provide essential services in the event of a significant incident may be valuable, but introduces unique questions related to governance, management, control and funding. Who will govern the core? Who makes decisions about attacks and how to respond to them? What are the standards required to interconnect and how will they be enforced? To answer these questions, it will necessary to engage the stakeholder community in a fashion that is engaged and representative of the diverse and localized nature of public safety. Workshops, working groups, collaboration, and R&D efforts

will be necessary to identify key requirements, develop governance models and implement a solution that is both secure and functional.

- NIST requested comment on how it should engage public safety practitioners and technologists as part of the planned R&D projects to ensure proper prioritization of efforts and effectiveness of developed solutions.

L.R. Kimball responds that the NIST should consider the creation of working groups and/or committees that engage stakeholders from within the public safety community. These working groups will bring real world expertise "from the trenches" helping to level set activities and set priorities Furthermore, the NIST should consider involving vendors as well as other stakeholders in "interoperability" plug fests or test lab environments where new configurations can be tested or tried.

Lastly, L.R. Kimball suggests that NIST construct and implement an effective Research and Development plan and process that identifies and captures the key core elements, features, and limitations as identified by all public safety related jurisdictions, agencies, and disciplines. Structure the R&D work to align and support successful implementation of the core program components. With sufficient research data obtained, enable NIST to align R&D priorities to effectively establish base line operational, functional and technical requirements.

In order to close technical gaps and obtain maximum benefit from the discovery phase of the research, the following approaches should be included.

- Conduct vendor and issue analysis as it pertains to the baseline requirements
- Compare and contrast public safety needs and requirements to existing commercial broadband systems
- Identify 4G LTE broadband assumptions and constraints and limitations from an operational, functional, and technical perspective. For example, public safety agencies

depend on radio to radio communications in remote and incident command situations that do not access the tower site infrastructure.

- Interaction, integration, and inclusion with other public safety initiatives such as NG9-1-1.
- Specific focus on the operational, governance and security issues of the technology.
- Avoid communications research that might overlap or create unnecessary duplication
- Conduct final audit to stakeholders on any areas that might have been over looked or are missing
- Clarify what portion of research if any, is dedicated to future voice capabilities
- With all the findings in place, identify what portion of existing LTE commercial infrastructure can be integrated into legacy public safety systems