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

Joint Comments of

the Palo Alto Research Center and

Motorola Solutions, Inc.

The Palo Alto Research center (PARC) and Motorola Solutions, Inc (MSI) appreciate the opportunity to provide comments on NIST's Public Notice[1] regarding possible research and development priorities for new features and capabilities of the nationwide wireless Public Safety broadband network. We hope that NIST will find these comments helpful in determining the technology areas that might be appropriate for investing research funds from the Public Safety Investment Fund (PSIF), part of the Administration's proposed Wireless Innovation (WIN) Fund, to advance the development of those feature and capabilities.

The submitters recognize the important steps that NIST has already taken to identify the unique wireless broadband communications operational requirements of the Public Safety community, over and above what is currently being deployed in commercial Long-Term Evolution (LTE)-based wireless broadband networks. We understand that these previously identified requirements, as detailed in the U.S. Department of Justice Community Oriented

[1] *See* Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network. NIST Docket No. 110727437-1433-01

Policing Services (COPS) report,[2] are to be used as a starting point to identify possible areas of investment of PSIF funds to "conduct R&D to support new standards, technologies and applications to advance Public Safety communications".[3] Both PARC and MSI support this effort, and are looking forward to working closely with NIST, the Public Safety community, and others in this market to identify and advance the development of the technology needed to support the current and future needs of Public Safety.

I. Prioritization of Research Projects

The existing Public Safety communications marketplace is a dynamic one, with many vendors actively working with representatives of the Public Safety community to develop solutions to meet the communications needs of first responders. As NIST undertakes the challenging effort to identify the priority areas for the advancement of communications technology needed by the Public Safety market, both short and longer term, the current efforts of technology development already underway in the Public Safety communications arena can provide substantial guidance regarding the areas of future research that will provide the most benefit to the Public Safety community.

The decision to base the Public Safety wireless broadband network on existing, standardized commercial technology (e.g. LTE) provides a substantial head start in making equipment available for immediate deployment. It also allows the significant amount of investment already being made by the private sector in researching future solutions for both the Public Safety and commercial networks to be leveraged, which allows the funding ($500 million) proposed for the PSIF to be focused on research areas that are consensus priorities, but which are

---

[2] *Id.* at 4
[3] *Id.* at 5

not already under development within the private sector. We believe an open and collaborative process, with close cooperation among the Public Safety community, the private sector, and NIST, is the best way to ensure that the most vital future communications needs, selected from the broad areas of possible research that have been detailed in the Public Notice, are targeted.

As these priority areas of research are identified and funded, we also believe it would provide the most benefit to the Public Safety community if the results of all PSIF-funded research projects are made broadly available to the private sector. Sharing the results of this research with the market will help ensure that the practical solutions will be deployed in support of Public Safety in the fastest and most efficient way possible.

II. Priority Research Areas

PARC and MSI agree that, as the COPS report illustrates, there are many potential priorities for advancement of public safety wireless broadband communications technology which would benefit from additional funding, many of which are already being addressed to varying degrees by private sector R&D activities. However, there are still some key areas in which the PSIF funding could provide significant benefit to the Public Safety community.

One mission-critical component of a public safety broadband network is how it operates at the edge of the network, where the handheld and mobile units are typically concentrated in support of first responder communications at an incident scene. This functionality is especially critical in these emergency situations, where the location and magnitude of such incidents is by definition unknown ahead of time, and is one of the key distinguishing features of Public Safety networks. Currently we are starting to see the deployment of LTE-based networks, which will combine the standardized network management and operational capabilities already being used

in commercial networks with the specific deployment requirements, site hardening, functionality and applications required to meet the unique needs of the Public Safety community.

LTE will provide much of the functionality needed for the networks being deployed by Public Safety today. However, in the future the functionality of a Public Safety network may be enhanced if the capability of operating in a distributed manner, without any central infrastructure, can be added to the existing network-based operation to deal with emergency situations where network-based communications is not reliably available. In these scenarios, the network must be autonomous, delay and disruption tolerant, and allow the users at the edge of the network to get the job done even if working in isolation. Users of the network must be able to exploit any data already in the network and not require a robust backhaul to centralized servers or the Internet to ensure some level of communications support even when access to network-based data or resources are temporarily not available.

A broadband Public Safety network should not be limited to the core services of voice and text telemetry alone at times when the infrastructure is unavailable. Command and control systems are relying on multi-modal information-centric tools more and more every day and need the infrastructure to support this. Different tools may require anything from low rate position tracking to high bandwidth multimedia transfers. Each application should be able to signal to the network its specific data communications requirements in order to assist the network in managing mission critical traffic, and planning resource usage. One should be careful to note that this management and planning cannot rely on centralized control and authorities but at the same time must be able to be part of the more complex global system. In the Public Safety environment, dynamic control and prioritization by an incident commander or his/her designee is

extremely important, as priorities are event driven, and may change rapidly during the course of managing a prevention or response activity.

Due to the nature of emergencies, Public Safety cannot plan ahead for every possibility. This is true for coordination of first responders and it's true for coordination of networks. Sometimes Public Safety communications requires heavy video streams, other times an increase in voice calls or access to database information is needed. The physical environment is also important, as sometimes responders will have a strong signal available, and at other times Public Safety operations could be underground with very low signal strength. Adding the capability for the system to make distributed decisions will enhance the first responder's ability to deal with real disasters. The strength of a public safety communication system will be tested not at a regular traffic stop, but after an earthquake, terrorist attack or tsunami. However, it is also important to recognize that, for Public Safety, even a routine traffic stop could quickly turn into a situation of life and death, demanding the best communications solution possible.

We need to enable each responder's device to help make localized decisions based on each device's context, and what the device knows about its network surroundings and peer devices. For example, each device can track the condition of the radio environment. If a particular channel is nearing capacity, alternate channels could be used, if sufficient spectrum is available. Devices should also support multiple networks and allow concurrent network access. A handset should be able to access local 3G or 4G networks, when available, but also operate in local mesh networks. Localized decisions can then be taken on what network to use, optimizing the routing of voice, text, and data. This would allow local, high speed data access among the nearby users, offloading the backhaul network. At the same time it would ensure continued local group operations even when the backhaul is not available.

As stated above, we believe future public safety networks will be multi-modal, carrying voice, text, audio, video, images and data; some real-time and some not. An image by itself might not be very informative. It is the context and meta-data associated with it that gives it real value. We believe this same concept should be applied to the network as a whole. In order to contextualize the information and relate one piece of data to another, we must have an information-centric view of the network. Data from one application should be compatible with data from other applications. For example, we might have a location service that keeps track of each responder's position, as this data could be very useful for a mapping application that quickly shows an incident commander or dispatch/command center personnel the location of all responder resources. It is also potentially useful for an application that finds the nearest person with training in chemical fires, so the most effective resources could be identified and sent to the scene of a fire more quickly.

We can imagine many of the applications that will be built for a future multi-modal public safety network, but we can't imagine all possibilities. This means that we must design a clean and extensible API that will allow new applications to be created and take advantage of the data exchange capabilities even when each application is developed independently.

In summary, we believe future Public Safety broadband networks should offer:

- The ability to use the existing (and planned) infrastructure, including LTE
- The ability to communicate in a decentralized, peer-to-peer and multi-hop manner for voice, video and data
- The ability to tolerate high delay and disruption of the wireless connection to command centers and the Internet
- Autonomous devices that can adapt to the current conditions and use the best network (including LTE and mesh) for the situation
- Data abstractions for producing, sharing and consuming data at a global system level
- Communications abstractions so applications can communicate and share data without needing to know where the data or recipient is

III. Edge Networking Scenario

This section describes a potential scenario to help illustrate the benefits that future enhancements addressed in these comments could bring to Public Safety broadband network operation.

At 6pm on a Thursday afternoon, a 6.8 magnitude earthquake strikes the east coast with an epicenter a few miles south of Manhattan. Police, fire, and medical personnel scramble to deal with injuries, deaths, hazards, damage, and potential vandalism. Numerous separate units with different areas of specialization across several jurisdictions will all respond to the variety of problems. Key to the effectiveness of their response is a system that creates clear, rapid communication and coordination among the multiple entities involved.

Let us consider one particular event that could result from this scenario: A train has derailed in a tunnel running under the river between Manhattan and Brooklyn. At the west end, the tunnel has collapsed. At the east side, water has started to leak in. The water coming in will make it hard to evacuate in that direction. Swift action is needed. A crew of New York City's Transit Authority personnel work with the Fire Department, City of New York (Team A) to clear rubble in order to open the collapsed tunnel. Meanwhile a group of emergency medical technicians (Team B) enter the tunnel from the Brooklyn side and makes its way towards the train. Underground communication lines have failed. Deep in the tunnel there is no way to receive radio signals from the surface, so while connection to the Public Safety broadband network is not possible, it is still possible for the handheld devices carried by the responders to communicate directly with each other. Leveraging this capability, Team B communicates

amongst themselves, their devices working independently of access to the Public Safety broadband network at the surface. The responders have cached information before becoming disconnected and can detect and talk to the other devices around them. They reach the train and first group of victims. Two team members (B1, B2) stay with this group to deal with the most seriously injured passengers. Their handheld devices are not connected to external networks but they can still communicate with the rest of the team, consulting each other on what needs to be done next. Most of the interaction between team members is by voice as B1 and B2 perform triage.

Team A continues to the next car and two more team members (B3, B4) stay behind to deal with more wounded people as the remaining two (B5, B6) make their way to the end. B5 and B6 notice a victim trapped under the rubble at the end of the tunnel. They realize that Team A needs to be aware of the victim as they are clearing the rubble.

B5 snaps some pictures and records a short video report of surroundings. He needs to get this information to Team A. Talking via radio, B5 tells B1 (who is closest to the east end) to go deliver the information. After verifying that she has received the pictures and video, B1 runs back towards the east side of the tunnel. In a few hundred yards her device informs her connectivity has been re-established with the main Public Safety broadband network. Data starts being uploaded to the central command center. B5 is now able to talk to dispatch and give an update on the situation.

B1's handheld device is just barely within reach of the Public Safety broadband network, but luckily she's also in range of the rest of her team. Her device immediately starts acting like a relay node. With some communication reestablished, the other team members can now send and

receive data. Due to the long distance, the radios can only deliver low bandwidth so data is prioritized. B1 leaves her radio behind (to maintain the communication) and returns to the train to continue providing medical assistance.

B5, who is with the victim under the rubble, can now establish a video call to Team A at the other side. Because bandwidth is low, the quality is extremely low. The system prioritizes audio followed by as many images as possible. B5 coordinates with Team A on how to create a small opening, and eventually they are able to break through without harming the trapped victim. The radios can now detect each other and start communicating directly. B5's video will now be sent in high-definition to Team A. All of Team B now starts relaying via B5 and B6's radios. The two teams will now communicate directly to create a large enough opening to start evacuating victims.

IV. Research Agenda

A government funded research program should focus on areas of high importance to Public Safety objectives that would otherwise receive little commercial investment due to their specialized needs. We have provided the above scenario to illustrate some of the unique situations faced by first responders, in order to help identify possible areas of research that could advance Public Safety communications technology. This section discusses these areas and suggests several potential research projects. The autonomous operation of devices in a mesh network with little or no connection to the main Public Safety broadband network is a key future enhancement and differentiator of Public Safety networks from commercial wireless systems. Important topics for potential research to support this future enhancement include the self-organization of devices into efficient network topologies to transport multimedia traffic over

multiple hops, and scaling of the ad hoc network to support many devices through dynamic channel use. Such a system would need to include mesh-aware QoS mechanisms to find suitable paths in the mesh environment efficiently, and to reserve bandwidth in accordance with available priority mechanisms.

Developing standard network communication and storage mechanisms that help exploit mesh capabilities when devices are disconnected from the main Public Safety broadband network and command center is also a critical future enhancement. When not connected to the main Public Safety broadband network, responders should be provided the ability to share text, voice, video, and documents among themselves in isolation from centralized servers and facilities.

V. Summary

PARC and MSI again applaud the efforts of NIST to support the communications needs of the Public Safety community, and to help advance the state of wireless broadband communications technology through investment in priority research projects via the proposed PSIF. We urge NIST to adopt an open and collaborative process to ensure that ongoing development efforts by the private sector are taken into account when these priorities are identified, and PARC and MSI look forward to being active participants in that process. With a significant amount of investment already being made in Public Safety broadband communications technology, we believe that appropriate areas can be identified which, when enabled by PSIF funding, could significantly advance the state of Public Safety communications, without duplicating the efforts and investments of the private sector in this critical area.