The National Institute of Standards and Technology (NIST) Request:

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[Docket No.: 110727437–1433–01]

Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice and request for comment.

SUMMARY: The U.S. Department of Commerce's (DoC) National Institute of Standards and Technology (NIST) is seeking input on various possible features of a new nationwide interoperable public safety broadband network. This input will be used by NIST to help determine research and development priorities in anticipation of the President's Wireless Innovation (WIN) Fund to help drive innovation of next-generation network technologies.

DATES: Comments are requested by 5 p.m. EDT on October 12, 2011.

ADDRESSES: Comments should be sent to Dereck Orr, *dereck.orr@nist.gov*.

FOR FURTHER INFORMATION CONTACT:

Dereck Orr, Office of Law Enforcement
Standards, National Institute of Standards and Technology
325 Broadway, Boulder, Colorado 80305,
Telephone number: (303) 497–5400.
E-mail address: *dereck.orr@nist.gov*

In reply to the NIST request above, California Technology Agency Public Safety Communications Office is pleased to offer the following "feature" and request question related responses on the following pages. Some features or feature request questions have been intentionally left blank. Thank you for the opportunity to participate.

RESILIENCY: The ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   Currently, the California Technology Agency Public Safety Communications Office (PSCO) owns and operates a highly robust statewide microwave network (≈99.999% or better reliability) for its state, local and federal public safety customers. PSCO also has a maintenance organization comprised of telecommunications technicians distributed throughout CA which not only maintains the microwave network, but all state agencies public safety radio communications systems and subscriber equipment as well. As a result, the mean time to repair (MTTR) for these systems and equipment is low; that is, outages are expeditiously addressed.

   Whereas public safety has not had significant exposure to wireless data networks, it has not yet faced the implications of poor resiliency. It is reasonable to assume, however, that public safety will develop an increasing reliance upon data features and functions with exposure, and that the availability of these resources will be critical to life safety. As such, public safety broadband network *resiliency* should be comparable to the high expectation public safety has of its current telecommunication technologies.

2) Current gaps that exist preventing the realization of the full potential of the feature;

   Since the public safety industry is currently in its infancy with respect to practitioner use of broadband technologies and applications and a nationwide public safety broadband network does not currently exist, the gaps to achieving *resiliency* are speculative. It is, however, reasonable to

assume that comparable lessons can be drawn from the local, regional and state public safety communications system models established throughout the nation. That is, policies and procedures which accommodate resiliency have been established and are practiced for current public safety communications networks. Slightly modified versions of these should suffice for the subject national public safety broadband network. In the case of the State of CA, PSCO has the facilities, resources (i.e., test equipment, etc.), skills and staffing necessary to sustain a high degree of network, systems, and equipment *resilience*.

3) Possible research and development that could take place to close any technical gaps;

   Investigate and follow the models discussed in PSCO's response to (2) above.

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

   Challenge A: Establishing not only a one-time funding allocation, but also a sustainable funding source.
   Challenge B: Establishing an attainable, yet dynamic model optimized to accommodate technological and application advances.

   On a local level, cities and counties enjoy more agility in coalescing multijurisdictional support, then accommodating short-range budgeting needs and long-range maintenance expectations with respect to public safety communications systems development, implementation, and maintenance. States have less agility in doing so. It is reasonable to assume that on a nationwide basis, it will be difficult to coalesce and

RESILIENCY: The ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements

maintain ubiquitous support across so diverse and dynamic a set of interests (needs) as those existing across the United States.

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

SELF-ORGANIZING: Self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   A Self-Organizing network (SON) is critical in the deployment of a nationwide broadband network. As the network builds out, SON removes the necessity of an organization to coordinate the deployment and maintain a database of stations and their operational configuration. The "Plug-N-Play" nature of a SON will facilitate a much more rapid and less costly deployment. The SON also facilitates self network reconfiguration to try to maintain service in the event of a failure in a portion of the network.

2) Current gaps that exist preventing the realization of the full potential of the feature;

   Long Term Evolution (LTE) currently incorporates a Self-Organizing function.

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

MESHING *(ad-hoc device-to-device communication):* A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   The current configuration of an LTE network relies on some form of backhaul from each node into the Core Network. Failure of a node's backhaul takes that node off line even though the Radio Access Network (RAN) is still operational. If the network had the ability to mesh, presumably the node with the failed backhaul could establish a mesh connection with neighboring nodes and continue to provide at least some level of service.

   At the user level, the ability to mesh between User Equipment (UE) could help facilitate two different functions. The first and simplest is a user to user (peer to peer) connection. This replicates the car-to-car, or direct mode of operation of existing land mobile networks. This function would allow communication between UE's in the absence of the network, whether due to network outage or being in an area where the network isn't built out.

   The second function would be as a relay in a true meshing configuration. In this condition one or more UE's would become in effect a repeater for a UE that can't access the network directly due to poor signal levels.

2) Current gaps that exist preventing the realization of the full potential of the feature;

   It appears that some mesh-like functionality is contained in 3GPP release 10 in the form of relay nodes. However this will not address the condition of no service to devices that are in poor signal areas where there are no

MESHING *(ad-hoc device-to-device communication):* A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network.

relay nodes available for connection, but there is connectivity to a nearby UE that does have network connectivity.

3) Possible research and development that could take place to close any technical gaps;

   Research and development of UE (peer-to-peer) mesh networking functions.

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

   Peer to Peer mesh networking may not be a desire or at least a priority for the 3GPP community. As public safety is using a set of standards developed for commercial users worldwide, it will be difficult for a small specialized set of users such as U.S. public safety to influence the direction that standards take in their development.

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

ADAPTABILITY: The ability of the network and/or device to modify/ change behavior based upon external conditions.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   The network must have the ability to adapt to special circumstances. Commercial Networks are designed based on a relatively uniform distribution of user devices. Public safety has a relatively uniform distribution until an incident occurs when a large number of users gather in a small area, potentially in one sector of one cell. This high concentration of users in one sector of one cell can easily overwhelm the network. The network needs to be able to adapt to the high concentration of users. Possible results could be allocation of additional backhaul resources via the reassignment of users not assigned to the incident to neighboring cells or beam forming of neighboring cells/sectors to pick up some of the increased traffic load.

   At the user level, devices that can adapt to network loading or network unavailability and switch to a mesh architecture to operate in a peer to peer mode, passing traffic off network. This can either be a one to one, or a one to many scenario at the incident where access to the network is not needed, or traffic passed from a device that can’t access the network to a device that can access the network.

2) Current gaps that exist preventing the realization of the full potential of the feature;

   This type of adaptability and or functionality is not currently available in the 3GPP standards. 3GPP Release 10 provides some of the functionality that might be needed (beam forming) but is not currently accepted as the base standard for public safety.

ADAPTABILITY: The ability of the network and/or device to modify/ change behavior based upon external conditions.

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

PRIORITIZATION: The ability to prioritize network traffic based on assigned priority schemes.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   The public safety broadband network must have prioritization as one of its system features. Priority assignment must be based on both a resource type and an applications type. For example, A law enforcement patrol unit has priority over a parking enforcement unit. A law enforcement user running a license plate needs to have priority over another law enforcement user downloading forms or uploading a report. Video must have priority over data. Emergency button activation must have the highest level of priority.

   Priority assignment must be dynamic. A law enforcement officer that is a member of the SWAT Team needs to have a higher level of priority when assigned to a SWAT detail than when on normal patrol. An out of jurisdiction unit should have one level of priority if just visiting, but have a higher level of priority if on assignment as a mutual aid response. Priority assignments should be both user driven and network driven. Activation of the emergency button or requesting a drivers license check are user activated priority assignments. Assignment to a SWAT detail or out of jurisdiction mutual aid responder would be a network assigned priority level.

2) Current gaps that exist preventing the realization of the full potential of the feature;

   Due to the fact that LTE is a standard developed for commercial networks, it is doubtful that dynamic priority assignment such as that needed by public safety is in the standards.

PRIORITIZATION: The ability to prioritize network traffic based on assigned priority schemes.

3) Possible research and development that could take place to close any technical gaps;

   Standards for implementing and managing priority levels will need to be developed, this would likely have to be done outside of the 3GPP standards, and handled at the network level.

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

   As LTE is a standard based on commercial network needs, implementing a priority level set of standards within the 3GPP community may be difficult at best, impossible at worst.

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

QUALITY OF SERVICE (QOS): The set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks. The goal of QoS is to provide preferential delivery service for the applications that need it by ensuring sufficient bandwidth, controlling latency and jitter, and reducing data loss.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

STRONG, DYNAMIC ACCESS CONTROL: Access control lists can be configured to control both inbound and outbound traffic on networks and authentication/verification of users/devices on the network.7 The level of access control should be sufficient to allow for entrée into a broad set of systems and databases needed by public safety (*e.g.,* criminal history databases, medical records, public work records, *etc.*).

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

***COMPATIBILITY WITH COMMERCIAL INFRASTRUCTURE**:* The utilization of a variety of commercial services when public safety is in areas not covered by the public safety broadband network.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   The capability to roam onto commercial networks is an important feature for those units that are outside coverage of the public safety network. The typical roaming condition would be for users traveling outside of the network, such as while responding to an out of jurisdiction incident. The ability to access the network and have at least some level of service and/or features is necessary when away form the home network. It is not reasonable to deny service if the only service available is the commercial network.

   The public safety networks however, must be designed to minimize the potential for roaming while within the network coverage area. The public safety network must be designed so that signal levels are high enough that user equipment is not likely to roam to the commercial network due to higher signal levels from the commercial network.

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

NETWORK SHARING: The shared use of infrastructure between commercial and public safety users.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   Shared use of infrastructure is desirable from a funding point of view. If commercial network providers have already developed sites to cover their users it is logical to make use of those same sites to provide service to public safety users in the same area. The resiliency of the sites however can vary greatly from what public safety requires. Public safety cannot accept sites that go down eight hours after the loss of commercial power. Will commercial providers be willing to upgrade their site standby power to support public safety needs?

   Shared use of commercial network backhaul also requires a high level of reliability and security from outside intrusion. Can public safety be assured that the commercial backhaul network is secure? If Core networks are shared can public safety be assured of the core's security?

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

   Site security is an aspect of site sharing that can be troublesome. Commercial providers may (and in various cases do) want to limit access to their equipment to their own staff. This can create problems if the site owner requires that anyone accessing their site is escorted by an

employee of the site owner. During wide scale, long term events, such as floods, hurricanes, or earthquakes, public safety cannot be denied access to a site to make repairs to public safety equipment due to the site owner not being able to provide escort to the site due to their own network problems. Commercial providers sharing site infrastructure must be willing to allow unimpeded access to the sites 24/7 and must be willing to make any upgrades to the infrastructure to provide the network reliability that public safety requires.

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

MULTI-MODAL: The ability of the network to support voice, video, data, and multimedia simultaneously.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   The network must be multi-modal. The network must be able to accept, and user equipment must be capable of processing, multiple modes of operation. Law enforcement needs to be able to send live streaming video from a dash camera while processing license plate and driver license searches. Emergency Medical providers need to send live streaming video of a patient while at the same time sending telemed data as the EMT is in voice consultation with the hospital.

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

SCALABILITY: The ability of a system, network, or process to handle growing amounts of work in a graceful manner or its ability to be enlarged to accommodate that growth.8 At the design phase, this could include requirements to ensure that scalability can be achieved, to the extent possible, by software enhancements and upgrades as opposed to by hardware replacements. Scalability also includes the need, in the case of a large scale event, to accommodate a rapid increase in the number of users in a limited geographic area.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

POWER AWARENESS: The ability of network/devices to control power functions.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

STANDARDIZED COMMON INTERFACES: Protocols, Application Program Interfaces, application platforms, radio capabilities, etc. that allow for competitive provisioning.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   Although the bulk of the network's use will be by resident practitioners within a localized geographic area, a significant network value will be its ability to support those same practitioners anywhere else in the U.S. – and to interoperate with practitioners within the confines of the new location in a predictable manner. This 'non-resident' access can only be achieved if nationwide governance and the local networks oblige.

   All user equipment must have a base level of standard functions and features. While in the commercial market, consumers may be willing to accept devices that don't support certain file formats where other devices do, public safety must be assured that all devices work in a consistent manner nationwide and that all devices support all the necessary file formats nationwide otherwise interoperability is not possible.

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

UNIFORM, UNIVERSAL ACCESS: The ability to access the network and data anywhere at any time through any device.

1) Assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

   (First Paragraph same as response (1) to STANDARDIZED COMMON INTERFACES)
   Although the bulk of the network's use will be by resident practitioners within a localized geographic area, a significant network value will be its ability to support those same practitioners anywhere else in the U.S. – and to interoperate with practitioners within the confines of the new location in a predictable manner. This 'non-resident' access can only be achieved if nationwide governance and the local network oblige.

   In PSCO's response to Question (7), we recommend that a fundamental set of common functions should be maintained across the network. That would seem to apply here as well.

2) Current gaps that exist preventing the realization of the full potential of the feature;

3) Possible research and development that could take place to close any technical gaps;

4) Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

   Public Safety Communications occupies a small market niche in the vastly successful telecommunications industry. Consumer demand and bottom-line returns drive the industry – and not in an altogether inappropriate direction for public safety. Many of the evolving features and functions available to consumers today can (and do) benefit public safety practitioners. …and their price point is attractive.

UNIFORM, UNIVERSAL ACCESS: The ability to access the network and data anywhere at any time through any device.

Public Safety must keep economic realities in the forefront as it launches forward in the development of its private nationwide public safety broadband network. Very affordable consumer products currently embody not only in vogue, but also useful advanced features and functions, and commercial providers currently offer services where economically advantageous. We should temper our expectations accordingly to the extent practicable.

It should be kept in mind that accommodating features and functions unique to public safety comes at a premium (necessarily passed on to public safety), and if the cost of end user technologies is outside the reach of practitioners nationwide (including those in rural settings), the level of participation will be impacted.

Similarly, if the network provider in a geographic region realizes too low a rate of return (due to low subscriber counts), it is unsustainable. …and yet universal access dictates its presence there.

5) Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

Additional NIST Questions

Additionally, NIST is requesting input on the following further considerations for the nationwide public safety network:

6) What is the importance of employing open standards for the nationwide public safety network?

   The public safety broadband network should extend ubiquitous, seamless use to public safety practitioners from other locals around the nation on an as authorized and as needed basis.

   If a rural county in Northern CA employs a proprietary technology not embraced by the national network or end-user subscriber equipment used elsewhere, their system will likely not be accessible by out-of-county resources – and their resources will likely not be able to access the network outside the county.

7) What is the need, if any, for commonality of functions across the system?

   A fundamental set of common functions should be established across the system, but additional functions should be allowed to be established on a local level to allow for requirements unique to the area. That is, Los Angeles may have a need for costly advanced features and functions not needed or affordable in a rural setting.

8) What is the importance of a multivendor environment for the network and what are the lessons learned in deploying a multi-vendor environment from the cellular and other industries?

   The system rates and subscriber equipment able to support the fundamental set of common functions advocated in response (6) must be affordable at the lowest economic level. This is unachievable when

accommodated by one vendor. Experience has revealed that as the number of vendor participants increases, the costs decrease.

9) What can be done to ensure both short- and long-term affordability of the network for all types of public safety agencies?

Under PSCO's response (4) for the "Resiliency" feature, we noted two requirements to maintaining resiliency in the short-term and long-term public safety broadband network:

A: Establishing not only a one-time funding allocation, but also a sustainable funding source.

B: Establishing an attainable, yet dynamic model optimized to accommodate technological and application advances.

Within PSCO's response to (7) and (8), we infer that affordability dictates that the network accommodate low cost subscriber units at a minimum able to support a fundamental set of common functions. This will render subscriber unit costs in areas of low population density more affordable. The low population density network should be able to accommodate more feature-rich public safety resources should the need for outside help arise – if only to support the fundamental set of common functions determined at a national level. Likewise, the more affordable subscriber units outfitted only with support for the fundamental set of common functions should be able to function on the public safety national broadband network within a high population density area should the need arise.

10) In a recent report, the President's Council of Advisors on Science and Technology 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 how NIST should pursue this recommendation. 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.

11) What is the marginal cost of the feature/functionality versus equipment available today?

12) 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?

13) How should NIST 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?

Typically, the public safety practitioners and technologists involved in any large-scale endeavors comprise representatives from economically solvent areas – not low population density areas – and yet low population density areas comprise the bulk of the geographic areas to be traversed by the national public safety broadband network. To optimize the use *and usefulness* of the evolving network, input from these ‘rural’ settings must be solicited, and the pragmatic input that is received must be carefully considered in the network’s development accordingly.