Before the
Department of Commerce
National Institute of Standards and Technology

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

COMMENTS OF
THE NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL

The National Public Safety Telecommunications Council (NPSTC) submits these Comments in response to the National Institute of Standards and Technology (NIST) request in the above-captioned proceeding.[1] In these comments, NPSTC recommends NIST focus primarily on those areas that require research, not just proper deployment, and that any research and development program be planned and executed in close concert with the local and state public safety community and relevant industry experts.

[1] *Notice and Request for Comment: Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network, Federal Register, Volume 76, No. 176, September 12, 2011.*

The National Public Safety Telecommunications Council

The National Public Safety Telecommunications Council is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. NPSTC has promoted implementation of the Public Safety Wireless Advisory Committee (PSWAC) and the 700 MHz Public Safety National Coordination Committee (NCC) recommendations. NPSTC explores technologies and public policy involving public safety telecommunications, analyzes the ramifications of particular issues and submits comments to governmental bodies with the objective of furthering public safety telecommunications worldwide. NPSTC serves as a standing forum for the exchange of ideas and information for effective public safety telecommunications.

The following 15 organizations participate in NPSTC:

American Association of State Highway and Transportation Officials
American Radio Relay League
Association of Fish and Wildlife Agencies
Association of Public-Safety Communications Officials-International
Forestry Conservation Communications Association
International Association of Chiefs of Police
International Association of Emergency Managers
International Association of Fire Chiefs
International Municipal Signal Association
National Association of State Chief Information Officers
National Association of State Emergency Medical Services Officials
National Association of State Foresters
National Association of State Technology Directors
National Emergency Number Association
National Sheriffs' Association

Several federal agencies are liaison members of NPSTC. These include the Department of Homeland Security (the Federal Emergency Management Agency, the Office of Emergency Communications, the Office of Interoperability and Compatibility, and the SAFECOM Program; Department of Commerce (National Telecommunications and Information Administration); Department of the Interior; and the Department of Justice (National Institute of Justice, CommTech Program). NPSTC has liaison relationships with associate members, the Telecommunications Industry Association, the Canadian Interoperability Technology Interest Group, the National Council of Statewide Interoperability Coordinators and the Utilities Telecom Council.

NPSTC Comments

In its Notice and request for comment, NIST referenced the fifteen operational requirements as set forth by the U.S. Department of Justice Community Oriented Policing Services (COPS) office National Forum on Public Safety Broadband Needs report, August 23, 2010.[2] That COPS office report states:

> The forum was designed to convene key participants from the public safety practitioner community to help identify, discuss, and develop solutions and recommendations that will help accurately reflect public safety's *operational and business* requirements for a National Public Safety Broadband Network.[3]

The COPS National Forum report on page 2 also concluded:

> **WHAT PUBLIC SAFETY NEEDS IN AN EMERGENCY IS…**
>
> A public safety-controlled network with the ability to efficiently access and share accurate and timely voice and information* during all stages**of an event in any geographic location with the appropriate resources, interoperability, robust and reliable capacity, based upon the needs of the responders, and with the ability to dynamically scale to changes in the situation.
>
> * **Information**, as used here, includes structured data (i.e., database, spreadsheets, etc.) and large unstructured data (i.e., images, video, and multimedia files).
> ****Stages** of a public safety event include prevention, interdiction, response, and recovery.

[2] National Forum on Public Safety Broadband Needs, August 23, 2010, http://www.cops.usdoj.gov/files/RIC/publications/e021111338-broadband-forum.pdf
[3] National Forum report at page 1

The COPS National Forum on Public Safety Broadband needs listed the following operational requirements that emerged from this event:

1. A dedicated high-quality network connection always available for sending and receiving continual data streams to support monitoring and resource tracking.

a. Automated vehicle location (AVL)
b. Alarm and critical infrastructure monitoring
c. Global positioning system (GPS)-enabled tracking devices
d. Intelligent transportation systems (ITS)

2. At a minimum, access to initial and updated basic incident information (voice- and text-based incident data).

a. Voice (radio) communications
b. Radio features should be consistent with current capabilities, such as APCO 16-like features (e.g., selective inhibit, emergency call button, etc.)
c. Computer-aided dispatch (CAD) incident data

3. An infrastructure that is hardened and secure, providing a high level of system availability.

a. Highly redundant
b. Self-healing
c. Protected from outside intruders or unauthorized access (intrusion prevention and detection)

4. When voice is converged, and in the event the infrastructure is compromised, public safety must retain stable and with clear voice communications.

a. Talk-around—ability to talk one-to-one and one-to-many (infrastructure-less communications)
b. Need optimal audio quality during adverse field conditions (background noise)
c. No latency on mission-critical voice

5. No geographic coverage limitations within the footprint of the National Public Safety Broadband Network.

a. Ubiquitous roaming on the public safety network
b. Coverage area model is based on geographic coverage versus population coverage
c. Equal to or better than current public safety land mobile radio coverage models

6. Dynamic management and control of the network.

a. Allocate available public safety bandwidth as needed
b. Add/remove users and grant network authorization
c. Upgrade network and devices and manage the timing and frequency of these upgrades
d. Define operational information and voice priorities dynamically and have the system process the information based on these on-demand priorities

7. Ensure interoperability with existing public safety-based systems.

a. Land mobile radio (LMR)
b. Private and public (commercially based) broadband systems
c. Nationally standardized interoperability access

8. Ability to send and receive large sources of information.

a. Geo-spatial data
b. Real-time video
c. Hospitals and patient information
d. Photographs (e.g., crime scene photos, mug shots, etc.)
e. Biometric information (e.g., fingerprints, facial, etc.)
f. Large files (e.g., PDF of preplans, building blueprints)
g. Mapping and orthophotography (aerial photography) information

9. A non-proprietary network based on industry standards.

a. Standards are required and not optional
b. Standards evolution must ensure backward compatibility

10. Single devices that support voice, video, and data.

a. Public safety grade is not a different base device, but is an enhanced version of a consumer-grade device with the ability to add features as required.
b. Ruggedized
c. Water-resistant and/or waterproof
d. Longer battery life
e. Intrinsically safe
f. Ease of operation/simple

11. Access to and from external information sources.

a. Internet/Intranet resources
b. Record access to databases (e.g., NCIC, fusion centers, etc.)
c. Hospitals and patient information
d. Traffic conditions

12. Easily integrates with other technologies.

a. Commercial networks
b. Satellite
c. Military technology
d. Standard-based networks and connectivity options (e.g., Wi-Fi, Wi-Max, RFID, Bluetooth, etc.)

13. Automatic management and control of the network.

a. Schedule automatic upgrades of the network and devices by predefined rules
b. Predefine operational information and voice priorities in advance and have the system automatically process the information based on these priorities

14. Current and future enhancements available to commercial consumers are provided to public safety with no limitations.

a. Device operating system upgrades
b. Apps and widgets
c. Accessories (e.g., Bluetooth, speaker microphones, batteries, etc.)

15. Ability to send, receive, and process information from the public (citizens and media).

a. Social media-based information (e.g., SMS, MMS, Twitter, Facebook, etc.)
b. Mass media feeds
c. Next Generation 911

In its Notice, NIST categorized the fifteen operational requirements from the COPS Forum report into the following four overarching themes: 1) resiliency; 2) availability and reliability; 3) security; and 4) affordability/commercial alignment. NIST then added some technical interpretation to the fifteen requirements, listed a set of related features and requested comments. The comments requested revolve around the importance of the various features, current gaps that prevent the full potential of each feature, possible research and development that could help close any technical gaps, any challenges that public safety could face and best practices from other industries that could be leveraged to expedite public safety's realization of these key features. NIST plans to use the input to inform decisions on a proposed Federal fund of $500 million to support research and development related to the public safety broadband network.

NPSTC believes it is important to establish that all the requirements set forth in the COPS Forum report are important. This Forum included a cross-section of urban, state, rural, and tribal public safety practitioners from law enforcement, fire, and emergency medical services. These practitioners came from around the country and included representatives from some of the 700 MHz broadband waiver grantees that existed at the time the Forum was held. As evidenced by the information gathered in the COPS Forum, and from previous NPSTC work on broadband requirements, the bottom line is that the total performance of the network is important. However, not all of the Public Safety broadband network requirements identified in the Forum report or in previous NPSTC broadband initiatives require government funded research and development.

For example, many of the requirements that NIST categorized under resiliency, availability and reliability can be realized through the deployment of existing LTE broadband technology using established engineering practices applicable to public safety requirements. These include designing

the system deployment for the proper coverage specified and ensuring the proper backup power and facility design and hardening to match the environment and potential disaster risks pertinent to the area in which deployment is being made. This category of requirements would benefit more from sufficient funding for deployment than from funding for research and development.

In addition, sufficient dedicated spectrum capacity is an essential foundational element for the proper reliability of the network, especially at incidents or events that routinely result in and increase of public safety communications traffic that must be supported. As the Public Safety community has unanimously and emphatically noted, Congress has the opportunity to support these needs by reallocating the D block spectrum to public safety to provide a total of 20 MHz of dedicated broadband spectrum at the outset of deploying the broadband network. It is spectrum, not research and development, that supports this requirement.

In contrast, discussion of these issues at NPSTC's recent quarterly meeting indicated that additional research and development would be valuable in other areas, for example, the area of security. Given a key benefit of the broadband network is to provide data access, there will be many points of connection to a variety of databases and information sources. Some of these databases and information sources will be maintained by Federal agencies, some by local or state agencies and some will be accessed from the public Internet. It is extremely important that to the maximum extent practicable, the public safety broadband network has virus protection specifically related to cross-contamination, i.e., application to application, as well as protection of network codes to prevent network wide attacks. NPSTC believes this is an area in which research and development could be beneficial.

Also, the discussion identified that it will be helpful to establish some best practices for agencies to have in pre-conditioning information before sending it over the network. Any pre-conditioning best practices of course need to consider how the information will be used and must meet public safety operational needs for low latency and immediate access.

NPSTC already has underway several Task Groups within its Broadband Working Group that are focusing on a number of the areas NIST has raised. These Task Groups benefit from participation by both knowledgeable Public Safety practitioners and multiple industry experts. Work is ongoing in Task Groups on Priority/Quality of Service, Local Control, and Security. NPSTC believes it is important to take account of this work before any future decisions regarding research and development are made.

NPSTC recommends that any government funded research and development also be put into the context of the overall picture for the Public Safety broadband network. The Public Safety community has already endorsed leveraging the commercial LTE standard and applying it in a public-safety grade deployment. The FCC has also incorporated the LTE standard interfaces into its rules as a requirement for the public safety broadband network. While there are still important decisions to be made, both the Public Safety community and industry are significantly down the path from a technology perspective in designing and planning initial deployments that can contribute toward public safety interoperability and operability to provide high speed data and video access unattainable on current voice networks. The LTE technology is also already being deployed by at least two major commercial operators in the 700 MHz band.

Accordingly, any research and development program funded under the proposed program should be a supplement to and not a pre-condition of the existing LTE standard and initial network deployment. The time frame to define research and development properly, conduct the research, test the results and commercialize products for the public safety environment could be substantial and should not introduce more delay in deployment of broadband capabilities for Public Safety.

NPSTC congratulates NIST for taking the lead to identify priorities at this early stage before the research and development funding is proposed but not yet a certainty. In addition, once firm decisions are made on the actual availability and amount of the funding, NPSTC recommends that NIST implement a close coordination with the Public Safety community and relevant industry

representatives to better define the research and development program. As discussed at the recent NPSTC quarterly meeting, it is important that any research and development be focused on public safety needs throughout the process.

Those funded to perform such research and development also need to be in close communication with Public Safety practitioner experts at the beginning of the process, not after conclusions are reached and the research path is already set. Also, while developments from other industries can sometimes be useful to Public Safety, the operational requirements of Public Safety must be paramount. As an example, the military had a significant set of legitimate requirements for its communications related to software-defined radios (SDR), and for years that defined much of the SDR research. However, while those requirements were legitimate for the military, they were not necessarily all applicable to public safety.

Conclusion

NPSTC wants to thank NIST for its assistance in helping to define beneficial research and development for the Public Safety broadband network. It is important that 1) close coordination with Public Safety practitioners and industry be maintained once the actual availability of research and development funding decisions are made; 2) any research and development be focused on areas where research is actually needed, not areas where existing engineering practices and operational experience already provide direction for deployments; and 3) the NIST work supplement rather than delay initial deployments of the broadband Public Safety network built off of existing LTE standard. NPSTC pledges its continued involvement to assist NIST in these issues important to the Public Safety community.

Respectfully submitted,

Ralph A. Haller, Chairman
National Public Safety Telecommunications Council
8191 Southpark Lane, Number 205
Littleton, Colorado 80120-4641
866-807-4755

October 12, 2011