One DHS Emergency Communications Committee Comments to the National Institute of Standards and Technology Notice and Request for Comment: *Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network,* Docket No.: 110727437-1433-01, 76 Fed. Reg. 56165 (Sept. 12, 2011)

The One DHS Emergency Communications Committee (Committee) is pleased for the opportunity to submit these comments to Docket No.: 110727437-1433-01. The Committee, which is composed of representatives from 22 U.S. Department of Homeland Security (DHS) Components and headquarters entities with emergency communications equities, serves as the principal forum for coordinating DHS emergency communications requirements, policies, and investments.

The National Institute of Standards and Technology (NIST) solicitation groups 14 features across the four themes of "resiliency in an emergency; reliability and availability; security; and affordability/commercial alignment." NIST requests that commenters identify the relative importance of these features and suggest research and development (R&D) and implementation measures that may be taken to advance the Public Safety Broadband Network (PSBN). The One DHS Emergency Communications Committee has prepared the following response to convey the Department's wireless broadband communications needs and perspectives as a partner on and potential user of the PSBN. The responses are organized around the four overarching requirement "themes" and additional "considerations" identified in the NIST request. The responses assume that DHS will be an eventual user of the PSBN or will leverage similar capabilities to those provided by the PSBN.

The first four responses below address the four "Themes" and corresponding "Features" provided in the NIST notice:

1. To ensure resiliency in an emergency

Resiliency: During catastrophic events or an attack on U.S. infrastructure, many DHS users would need to rely heavily on wireless communications systems to effectively carry out the Department's various response, recovery, and day-to-day missions. Currently, many DHS users utilize Component-owned or other shared Land Mobile Radio (LMR) systems as their primary means of achieving mission-critical wireless voice communications. These LMR systems are designed to continue to provide local areas radio frequency (RF) coverage independent of wide area network connectivity when network connectivity becomes unavailable, and are generally equipped with enough backup power to keep critical RF infrastructure running during a power outage until commercial power can be restored or additional backup power can be provided. Additionally, LMR devices can provide line of sight (i.e., talk-around) communications independent of RF infrastructure when this infrastructure is damaged or not accessible. DHS also utilizes a variety of deployable LMR solutions that enable rapid restoration or expansion of the networks as needed. Use of the PSBN or similar broadband network for mission-critical communications would require assured service levels and alternative modes of operation (e.g., failsafe, talk-around) to ensure operability in all scenarios.

Potential areas for R&D include—

- Hybrid devices or adapters that would enable LMR devices to operate on broadband networks, providing redundancy and additional coverage and capacity
- Hybrid devices or adapters that would enable broadband devices to operate on LMR technology and frequencies for access to LMR networks—for redundancy and improved coverage and capacity—and to achieve talk-around capabilities

Self-Organizing: The surging nature of DHS communications system usage and the integration of multiple agencies and services (e.g., voice, video, data) onto shared networks create challenges in providing users with required quality of service during all potential scenarios. These challenges are further exacerbated when part of a network is damaged or out of service. The ability for a network to self-organize to most effectively use available network resources is important for maximizing the availability and reliability of critical services, especially during special events, such as natural disasters, where increased network traffic may coincide with damage to the network. This includes the ability to integrate deployed nodes and integrate public and private networks to provide ad hoc solutions.

Potential areas for R&D include—

- Self-organizing network technologies that can utilize fixed and deployable network resources across multiple technologies
- Deployable self-organizing network nodes to extend coverage to areas that have no coverage from fixed networks
- Device technology to operate on multiple systems/bands (e.g., LMR, LTE) that may comprise a self-organizing network

Meshing (ad-hoc device-to-device communication): One of the primary challenges associated with using today's broadband communications technology for mission-critical communications is the lack of device-to-device capability, which is an essential feature provided by LMR. Meshing could be used to provide device-to-device capability when there is no infrastructure available due to network coverage limitations or damaged infrastructure. Meshing is also an important feature for extending access to fixed network resources into nearby areas that lack direct network coverage (e.g., in buildings and tunnels, surrounding areas beyond coverage footprint). However, spectrum availability and increased power consumption may present challenges for the implementation of meshing technologies. Additionally, use of broadband frequencies, which are generally higher than Federal LMR frequencies, could limit the range of meshing devices, which could impact practical usage, particularly if the technology is intended to replicate radio-to-radio LMR communications.

Potential areas for R&D include—

- Device-to-device mission critical voice communications capability through meshing
- Deployable mesh access points

Adaptability: The availability of wireless communications services varies greatly across DHS operational areas and scenarios. In major metropolitan areas, many systems and strong signals are likely available. In remote regions and areas with challenging terrain (e.g., mountain ranges), often few if any systems are accessible and coverage can be weak and spotty. Although the PSBN, as envisioned, will provide extensive coverage across the country, it will likely be cost

prohibitive to cover all potential areas where DHS users may require mission-critical communications. Additionally, major incidents can further reduce system availability as network resources can become damaged or saturated with traffic. In these instances, the use of alternative networks (e.g., commercial broadband, LMR) could be used to complement the PSBN. Adaptability of communications networks and devices is important to maximize system accessibility and availability within and across networks while optimizing power and battery life in all operational environments and scenarios.

Potential areas for R&D include—

- Multi-network (e.g., LMR, LTE, Wireless Local Area Network [WLAN]) prioritization and switching
- Session persistence and seamless roaming among disparate networks (e.g., LMR, LTE, WLAN, Commercial, Government)

2. To ensure reliability and availability

Prioritization and Quality of Service (QoS): Prioritization of network traffic and assured QoS is important to ensure successful delivery of the most critical information even when network resources are saturated. For DHS, mission critical voice communications are generally considered to be of the highest priority and require the highest levels of reliability and availability. Streaming video also requires high levels of reliability and availability in certain scenarios such as during a high-risk surveillance operation. Comparatively, many other data applications generally do not require this same QoS and therefore can sustain a lower level priority on integrated voice, video, and data systems.

In addition to prioritization of data types, prioritization among user types is also important. Currently, when conducting field operations, DHS users generally employ DHS-owned LMR repeater systems. DHS ownership and control of these systems eliminates the need to compete with other entities for priority access. If DHS users were to utilize a shared infrastructure with commercial or non-critical users, they would require that the system ensure sufficient access to meet mission-critical needs, especially during times of unusual network congestion (e.g., natural or man-made disaster, special security event). Specific protocols and priorities will also need to be determined to maximize user QoS when multiple critical users (e.g., DHS, public safety) require access during times of high network congestion.

Potential areas for R&D include—

- Data prioritization schemas and impact to applications under various scenarios
- Assessment of how various prioritization techniques, such as ruthless pre-emption and head of the queue, affect system availability under various scenarios
- Assessment of QoS requirements and impacts for various applications (e.g., voice, video, text, blue force tracking)

3. To enable security

Strong, Dynamic Access Control: Many DHS operations and communications are highly sensitive and require that information and system resources be protected from unauthorized access through authentication/verification of users and devices on the network. However, access

rights should also be easily and quickly configurable by authorized personnel to provide/withdraw ad hoc access to DHS users and partners and new devices as needed. Dynamic access control should restrict access as needed but not hamper interoperability, and must allow for the operation of certain applications independent of the network (e.g., device-to-device applications when network connectivity is not available).

4. To ensure affordability/commercial alignment

Compatibility with Commercial Infrastructure and Network Sharing: DHS users operate across large geographic areas of responsibility. Building and maintaining Federally-owned wireless communications systems that provide adequate coverage and capability across these areas has proven cost prohibitive. Although the PSBN, as envisioned, will provide extensive coverage across the country, it will also likely be cost prohibitive for the PSBN to cover all potential areas where DHS users may require mission-critical communications. Compatibility of Federal and non-Federal (e.g., PSBN, commercial) infrastructure would provide significant opportunities for cost efficiency through infrastructure sharing and integration. For example, leveraging non-Federal infrastructure in well served areas could allow DHS to focus its funding on extending coverage and capacity in underserved areas where DHS requires service. Public safety and commercial partners could also potentially leverage this additional coverage and capacity when needed. In addition to expanding coverage and capacity, this compatibility would reduce the cost of building in redundancy as the presence of Federal and non-Federal network resources could provide required redundant paths and capabilities. However, it should be noted that before the advantages of compatibility with commercial infrastructure can be realized, commercial networks must be able to provide the QoS, security, and reliability required for mission-critical communications.

Potential areas for R&D include—

- Seamless roaming across public safety and commercial networks, including maintaining common feature-sets and user experience
- Administrative and security partitioning over shared networks

Multi-Modal: DHS users require several types of mission critical information to support DHS field operations. DHS currently utilizes a variety of systems and devices to provide this mission critical information via voice, video, and data communications capabilities. Convergence of these capabilities onto an integrated network could reduce costs through the consolidation of infrastructure and services, and reducing the need for multiple user devices. This convergence could also result in more efficient use of spectrum resources. The challenges to a multi-modal network that must be overcome include demonstrating mission critical voice capabilities similar to that of LMR and ensuring the reliable prioritization and primacy of voice communications, over video and data, necessary to support DHS missions.

Potential areas for R&D include—

- Development of LTE mission critical voice capabilities and devices that meet or exceed the functionality and performance provided by current LMR technology.

Scalability: Given DHS's responsibility for disaster response, it is imperative to have a network that can accommodate a rapid increase in the number of users in a limited geographic area. For example, during and after a natural disaster or other large-scale emergency, DHS users often

must communicate amongst an increased number of responders temporarily located at or near the disaster/emergency area.

Power Awareness: DHS users often operate in the field for an extensive period of time without access to power outlets or battery chargers. While many mobile devices provide a sufficient battery life under normal conditions, battery life is significantly reduced with extensive use of applications and high-power operation in areas of in poor coverage areas. Devices must have the ability to control power functions to maximize performance and battery life based on network coverage, usage, and application requirements.

Standardized Common Interfaces: The diversity of DHS missions and the information and capabilities required necessitate standardized common interfaces in order to integrate a variety of devices, applications, databases, and systems onto a common network. Additionally, DHS users require dynamic access to future broadband networks and applications using their native devices to enable rapid establishment and de-establishment of interoperable capabilities as needed without the need to distribute additional devices or training when traveling or during an incident. Standard interfaces will allow for this dynamic access and for the development and use of customized capabilities that can leverage common networks and devices. Standardized interfaces will also allow for competitive provisioning of network resources to ensure the most critical capabilities are given the highest levels of service. Furthermore, employing common interfaces should help drive cost-efficiencies and vendor innovation through competition.

Uniform, Universal Access: DHS users require uniform access to future broadband networks and applications using their native devices to enable rapid establishment and de-establishment of interoperable capabilities as needed without the need to distribute additional devices or training when traveling or during an incident. DHS users also require seamless roaming and session persistence when traversing networks and geographies.

The following responses address additional "considerations" provided in the NIST notice:

5. What is the importance of employing open standards for the nationwide public safety network?

Open standards are imperative to achieving effective interoperability, information sharing, roaming across disparate networks, and cost savings through infrastructure integration and economies of scale. They also promote innovation and timely delivery of services to users, which may be critical to the prolonged success of the PSBN.

6. What is the need, if any, for commonality of functions across the system?

DHS users must often communicate with multiple partner agencies across multiple geographies and systems, sometimes with little time for pre-coordination. Commonality of functions and the use of standard technologies and configurations allow users to use their own devices when operating in other regions or with other agencies, enabling rapid establishment of seamless operability and interoperability, and reducing the need for additional ad-hoc training.

7. 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?

A competitive multi-vendor environment can help to improve innovation and cost through competition.

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

Building and maintaining large Federally-owned wireless wide area communications systems has proven cost prohibitive. However, by using the same standards, Federal, non-Federal, and commercial infrastructure could be integrated, allowing Federal funds to be focused on underserved areas while overall coverage, capacity, and capability are enhanced. Additionally, use of commercial or modified commercial devices could reduce equipment costs due to increased economies of scale.

In addition, DHS has invested significant funds in upgrading current wireless communications infrastructure and equipment. Therefore, the ability to reuse some of this infrastructure and equipment with new broadband capabilities could result in cost savings.

Finally, through the adoption of open architecture standards, the PSBN could ensure short- and long-term affordability. Open standards allow multiple vendors to offer product, improving cost competition and flexibility in implementing technology refreshes.

9. 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?

Scalable broadcast and management functions (talk groups): The ability to transmit and receive real-time voice messages and other information to and from discrete secure groups of users is required to enable the transition from LMR to broadband. Users require the ability to select the groups with which to communicate at any given time, as they would select a talk group or channel on an LMR system. The ability for administrators to dynamically create, configure, manage, and close down these user groups on an ad hoc basis is also required.

End-to-end encryption with over-the-air rekeying: Most DHS communications in the field are considered "sensitive but unclassified" and must therefore be protected by 256 bit Advanced Encryption Standard (AES) or stronger encryption in accordance with DHS security policy. Therefore, the ability to manage end-to-end 256 bit AES or stronger encryption across future broadband networks is critical for enabling secure internal and interoperable communications. The ability to remotely update and manage encryption keys through mechanisms such as over-the-air rekeying is also important to ensure the right users can communicate securely when needed.

Device-to-Device communications: The ability to communicate directly between multiple devices independent of network infrastructure is required similar to LMR talk-around capability.

Backwards compatibility of broadband devices with LMR: Compatibility between broadband and legacy LMR devices and infrastructure is required to maintain operational capability and maximize reuse of existing assets while transitioning from LMR to broadband systems.

10. 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?

NIST should continue to work with organizations like the Emergency Communications Preparedness Center (ECPC) for coordination with Federal agencies, who may be potential users of the PSBN.

NIST may also want to consider establishing a competitive multi-stage research, development, testing and evaluation program. Organizations like the Department of Defense, the Department of Energy, and major corporations use a multi-stage model for the development and procurement of products. Multi-stage contest can spur innovation and competition in the development of next generation mobile communications devices. If NIST chooses to establish this type of competition, it should coordination with other Federal agencies through the ECPC to ensure Federal requirements are incorporated.