To: Mr. Dereck Orr
NIST Office of Law Enforcement Standards
325 Broadway
Boulder, CO 80305
Phone: 303.497.5400

From: Kevin K. Gifford, Ph.D.
University of Colorado, BioServe Space Technologies
Engineering Center Rm. ECAE-1B08
Boulder, CO 80309-0429
Phone: 303.492.0299

Re: NIST Nationwide Public Safety Broadband Network RFI

Date: October 10, 2011

Dear Dereck –

Following, please find responses from CU-Boulder BioServe Space Technologies, in regards to the Department of Commerce National Institute of Standards RFI for Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network (PSBN) [Docket No.: 110727437-1433-01]

Responses are provided as requested in the RFI. Importantly, I wish to highlight two primary focus areas that we at CU-Boulder would suggest as strong candidates for future R&D activities in support of an operational PSBN:

1. Disruption Tolerant Networking for PSBN "off-network" operations where no communication infrastructure to the back haul network exists – this is not an uncommon search and rescue scenario.

2. Development of an information-sharing system (middleware) to enable the utilization of Public Safety information across disparate data producers and heterogeneous networks. This second feature recommendation is the most crucial missing feature from the current PSBN system in our opinion. Importantly, the development and utilization of a standards-based PSBN "middleware" will, in addition to enabling a truly unified Public Safety network, provide a transition pathway for the current extremely disparate multi-jurisdictional communications devices to the new PSBN. This capability protects the multi-billion dollar prior investment in legacy systems and enables a flexible, stage-wise transition to the PSBN for the awesome future.

Sincerely,
Kevin K. Gifford

Problem Statement: A candidate problem statement for the nationwide Public Safety Broadband Network (PSBN) is: *the PSBN shall provide the future communications infrastructure that enables public safety responders to perform their duties in the most reliable and cost-efficient manner available.*

This (self-composed, but pragmatic) is a far-reaching mission statement that necessitates several practical realities and design choices. Table 1 lists the U.S. Department of Justice Community Oriented Policing Services (COPS) identified public safety operational requirements.

For these fifteen operational requirements there are five fundamental technology-related capabilities that will provide the basis for successful, long-term, PSBN operation:

- Bandwidth (spectrum)
- IP networking: "thou shall be IP"
- Open Standards
- Commercial vendor participation
- Independent compliance assessment

Table 1 - COPS PSBN Operational Requirements
(1) A dedicated high-quality network connection always available
(2) Access to initial and updated basic incident information (voice and text-based incident data)
(3) An infrastructure that is hardened and secure, providing a high level of system availability
(4) Clear, stable converged voice operations: infrastructure-less voice, optimal quality, no latency
(5) Geographic coverage that has no limitations within the footprint on the national PSBN
(6) Dynamic management and control of the network
(7) Interoperability, including with existing public safety-based systems
(8) Ability to send and receive large amounts of information
(9) A non-proprietary network based on industry standards
(10) Single devices that support voice, video and data
(11) Access to and from external sources
(12) Easy integration with other technologies
(13) Automatic management and control of the network
(14) Current and future enhancements available to commercial consumers provided to public safety
(15) Ability to send, receive, and process information from the public

See COPS[1] for the full U.S. Department of Justice Community Oriented Policing Services (COPS) report. Following is a brief synopsis of how the fundamental technology capabilities directly relate to the COPS PSBN Operational Requirements:

(1) **A dedicated high-quality network connection always available:** Need sufficient bandwidth, need IP networking, need commercial infrastructure to supply network service.

(2) **Access to initial and updated basic incident information (voice and text-based incident data):** Network access provided by bandwidth, IP network, and commercial infrastructure. Ensure common standard for basic incident report records.

[1] http://www/cops/usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf

(3) **An infrastructure that is hardened and secure, providing a high level of system availability:** Leverage commercial infrastructure, leverage security services built upon IP standard capabilities of authentication, authorization, privacy and integrity.

(4) **Clear, stable converged voice operations: infrastructure-less voice, optimal quality, no latency:** Infrastructure-less voice (ad-hoc) is an IP-network provisioned capability, not a cellular capability; voice quality is influenced by available bandwidth, voice encoding, and quality of service provisioning (both an IP and cellular metric).

(5) **Geographic coverage that has no limitations within the footprint on the national PSBN:** The PSBN is utilizing commercial vendor network coverage. More vendors equal more coverage. The U.S. Government could (I would argue for "should") operate it's own separate public safety network infrastructure for back-up and "core" purposes.

(6) **Dynamic management and control of the network:** Commercial vendor network operation that will be augmented (maybe subsumed) by standard IP-network management services.

(7) **Interoperability, including with existing public safety-based systems:** Open standards, vendor-mandated participation, and compliance assessment program. *A fundamental capability missing from both the COPS and the PSCR feature list is that of information/application interoperability. This is crucial for seamless information exchange and utilization. IP is enforcing network interoperability but not information interoperability. This capability should be added to the PSCR feature list as a requirement.*

(8) **Ability to send and receive large amounts of information:** Bandwidth, IP networks, open standards.

(9) **A non-proprietary network based on industry standards:** IP network, open standards, compliance assessment.

(10) **Single devices that support voice, video and data (exchange):** IP networking, open standards, commercial vendor devices, compliance assessment for interoperability verification.

(11) **Access to and from external sources:** IP network with appropriate security provisioning.

(12) **Easy integration with other technologies:** IP networking provides the basis for network interoperability, open standards will facilitate integration with other (current and future) technologies.

(13) **Automatic management and control of the network:** Build upon / utilize the significant, well-tested, network management services for IP networks combined with cellular network management utilities.

(14) **Current and future enhancements available to commercial consumers provided to public safety:** Mandate to commercial vendors, open standards, IP-based applications from other (non public safety) market segments will be available.

(15) **Ability to send, receive, and process information from the public:** Public information transmission via IP, *still need to provide interoperable information capabilities*.

As requested in the RFI, Table 2 (below) summarizes our responses to the RFI topics. In a nutshell, building the PSBN on top of LTE, which includes IP networking, provides the PSBN the very important (crucial) advantage of leveraging the substantial IP-associated services of a robust network with integrated security, Quality of Service, and network management utilities.

Table 2 – CU-Boulder responses to the NIST Nationwide Public Safety Broadband Network RFI.

Feature	PSBN feature importance	Brief Comments	Commercial availability?	Available in relative short-term?	Current feature gaps to address	Possible R&D to close technical gap	Challenges in realizing potential of feature	Best practices from other industries
Resiliency								
Resiliency	Critical	DTN can help in this scenario for "off-network" operations	No	Yes	Disconnected operations	Advance RFC5050 DTN development	Video and audio streaming via DTN	Can leverage DTN capabilities and maturation
Self-Organizing	Critical	Yes, but not in a mutli-hop fashion	No, not really	Maybe: essentially network	Ad-hoc device comm. / bridge to back haul	Wide-area network autoconfiguration capabilities	Automated IP address management	Wireless sensor networks standard capability
Meshing	Critical	Via Wi-Fi, not via cellular	PAN, LAN IP meshing	Yes	Integrate with cellular backhaul networks	Wide-area network autoconfiguration capabilities	Automated IP address mgmt; power mgmt	Wireless sensor networks standard capability
Adaptability	High	Yes, but will likely evolve for PS						
Reliability & Availability								
Prioritization	Critical	Yes, policy more than mechanism	Yes	Yes	This is more a policy issue than a mechanism issue			
Quality of Service	Critical	Yes, policy more than mechanism	Yes	Yes	This is more a policy issue than a mechanism issue			
Security								
Dynamic Access Control	Critical	Yes, evolve for mobile PS purposes	Yes	Yes	This is more a policy issue than a mechanism issue			
Affordability & Commercial Alignment								
Compatability with commerical infrastructure	High	Want to leverage commercial R&D, infrastructure	Yes, with LTE and IP	Yes, with LTE and IP				
Network sharing	Critical	Want maximum available bandwidth for PS events	Yes, with LTE and IP	Yes, with LTE and IP				
Multi-modal communications	High	Integrated (single-device) voice, data, video	Yes	Yes				
Scalability	Critical	Peer-to-peer IP networks scale well	Yes	Yes				
Power awareness	High	Power is a resource; always want to conserve	Yes	Yes	Incremental gains from advanced algorithms	Advanced power monitoring with feedback evolution	Device scavenge power to augment battery level	Cellular / wireless sensor nets standard capability
Standardized common interfaces	Critical	Common interfaces make it easier for users to operate	Not across different hardware	With adequate R&D	Multi-platform, standards-based, middleware	Multi-platform, standards-based, middleware	Must be able to support legacy installation base	Use open standard - no proprietary solution
Uniform, universal access	High	Devices don't need to support all data types; can segment	For the most part - will advance	Yes	Multi-platform, standards-based, middleware	Multi-platform, standards-based, middleware	Must be able to support legacy installation base	Use open standard - no proprietary solution

We recommend considering two additional technologies to support the nationwide Public Safety Broadband Network: (1) Disruption Tolerant Networking, and (2) middleware.

Disruption Tolerant Networking: Radio Frequency (RF) spectrum allocation and wireless communications are the fundamental resources that enable Public Safety operations. Whether utilizing the current Land Mobile Radio based communication infrastructure or the future cellular/LTE/IP communications infrastructure there will be occurrences of "off-network" or out-of-network operations. Some example scenarios could include:

- Search and rescue operations in out-of-coverage locations and terrain
- Public safety operations in noisy, interference, prone areas
- Rescue operations interior to a building that prevents RF signal reception
- Operations in a locale where, for whatever reason, the cellular/LTE-based public safety network is unavailable

It is important to note not only the ample benefits of the Internet Protocol (IP) networks but also the limitations. Successful operation of the IP protocol depends upon the following four communication characteristics:

(1) An end-to-end network path must exist for the entire communications session

(2) Retransmission based upon immediate feedback from data receivers enables effective recovery from errors. The Transmission Control Protocol (TCP) depends upon low latency of transmission and feedback (on the order of hundreds of milliseconds) to function properly – it is essentially a control feedback loop.

(3) Small transmission bit error rates (BER); large error rates in noisy wireless links break TCP/IP.

(4) There are relatively consistent symmetric transmission rates between a sender and a receiver.

Mobile wireless communications have the potential to violate all of the above four terrestrial Internet assumptions. To overcome these limitations the Disruption Tolerant Networking (DTN) protocol has been developed to augment, and in some cases replace, IP. Importantly note that DTN can ride on top of IP – this is an often-utilized network stack strategy.

What is DTN? DTN is a set of protocols that act together to enable a standardized method of performing store and forward communications. DTN operates in two basic environments: low-propagation delay and high-propagation delay. In a low-propagation environment such as may occur in near-planetary or planetary surface environments, DTN bundle agents can utilize underlying Internet protocols that negotiate connectivity in real-time. In high-propagation delay environments such as deep space, DTN bundle agents must use other methods, such as some form of scheduling, to enable connectivity between the two agents.

The protocols that make up the DTN protocol suite are documented in the following RFCs and Internet Drafts:

- RFC4838 – DTN Architecture
- RFC5050 – Bundle Protocol Specification
- RFC6257 – Bundle Security Protocol
- RFC5326 – Licklider Transmission Protocol – Motivation
- RFC5326 – Licklider Transmission Protocol – Specification
- RFC5327 – Licklider Transmission Protocol – Security Extensions
- draft-irtf-dtnrg-bundle-eidrefs – draft version 01
- draft-irtf-dtnrg-cbhe – draft version 02
- draft-irtf-dtnrg-bundle-metadata-block – draft version 03
- draft-irtf-dtnrg-bundle-metadata-conf – draft version 01
- draft-irtf-dtnrg-bundle-encapsulation - draft version 05
- draft-irtf-dtnrg-bundle-previous-hop-block - draft version 07
- draft-irtf-dtnrg-bundle-retrans-block - draft version 05
- draft-lindgren-dtnrg-prophet - draft version 02

For the Public Safety Broadband Network that is fundamentally based upon wireless transmission, DTN store-and-forward improves the **resilience** of the wireless communications. The store-and-forward nature of DTN is an effective approach to communicate in disconnected, or highly stressed (intermittently connected), environments[2]. DTN supports emergency notification broadcasting[3]. DTN can make use of the concept of opportunistic forwarding to achieve more reliable communications in emergency situations[4].

Middleware: The fundamental recommendation to the Department of Homeland Security (DHS) regarding communications lessons learned resulting from Hurricane Katrina is:

LESSON LEARNED[5]: The Department of Homeland Security should review our current laws, policies, plans and strategies relevant to communications. Upon the conclusion of this review, the Homeland Security Council, with support from the Office of Science and Technology Policy, should develop a National Emergency Communications Strategy that supports communications operability and interoperability.

---

[2] Fall, K., "A Delay-Tolerant Network Architecture for Challenged Internets", *SIGCOMM '03 Conference Proceedings: Applications, Technologies, Architectures, and Protocols for Computer Communication*, 2003, pp. 217-34.

[3] Kutscher, D., Greifenberg, J., and Loos, K., "Scalable DTN Distribution over Uni-Directional Links", *ACM SIGCOMM Wksp. On Networked Systems for Developing Regions*, Japan, Aug. 2007.

[4] Shanmugam, M. et al, "Emergency Services in Delay Tolerant Environments", *64th IEEE VTC,* Sep. 2006, pp. 25-28.

[5] http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/chapter5.html

The fundamental problem for a PSBN Unified Communications system is the disparity of devices that will utilize the PSBN and the potential for multiple heterogeneous communications links (multi-band radios or multi-radio transceivers). Simple data exchange suddenly becomes much more problematic when vendor devices transmit simple sensor readings such as temperature in a variety of byte-wise formats. Standard messaging must be utilized so that senders and receivers (publishers and subscribers) can exchange data. Even more important is the ability to exchange information – this capability is not addressed in the NIST Nationwide Public Safety Broadband Network RFI.

A properly designed middleware provides many features that will be of benefit to the PSBN as summarized in Table 3.

Table 3 – Features and Benefits of middleware applicable to the PSBN

Feature	PSBN Benefit
Protect legacy equipment investment	Provide a transition pathway for the extremely disparate multi-jurisdictional communications devices to the new PSBN. Protects the multi-billion dollar prior investment in legacy systems[6] and enables a flexible, stage-wise transition to the PSBN that can be managed
Information Interoperability	Provides application information interoperability so all applications can make use of published data automatically and with no special processing
Multi-vendor Solution Set	Multi-vendor hardware and software can be considered for the engineering solution – both proprietary and non-proprietary
Mobility	A properly design network-aware middleware either helps, or directly enables, seamless IP-network roaming of equipment, communication devices and personnel
Scalability	Peer-to-peer distributed publish/subscribe architecture enables highly scalable systems from tens of devices to thousands of data producers
Network robustness and Reliability	A middleware can automatically reconfigure to enable entire sub-networks to enter or leave the PSBN network; operation can continue in a partitioned network, enables networks to automatically recombine
Platform Independence	The middleware can run natively on multiple operating systems and hardware
Ease of Application Composition	Middleware helps to enforce conceptual integrity of overall system, software development kit (SDK) aids development programmers to easily build user applications
Integrated Security	A middleware should provide, and/or have the ability to utilize network stack services for authentication, authorization, integrity and privacy
Endpoint Reprogrammability	Endpoint communication devices can be selectively (or group-wise) chosen and dynamically reprogrammed to upgrade functionality while maintaining nominal PSBN operational status

[6] SAFECOM, Statement of Requirements for Public Safety Wireless Communications & Interoperability, *Department of Homeland Security*, Version 1.0, pp. iv, March 10, 2004.

DataVac: A final suggestion for PSBN consideration is the "DataVac" concept. A DataVac is a mobile (PDA-like) device and data store that can store ("slurp") data from PSBN networks, and hold the data until a downstream path-to-destination is determined in the event an immediate network path does not exist. The DataVac employs three fundamental technologies:

1. Software Defined Radio for RF transmission agility
2. Disruption Tolerant Networking for store-and-forward network operations for connected and intermittently connected operational scenarios
3. Publish/subscribe middleware to enable Public Safety information exchange and to enable a truly unified Public Safety network;

The NIST Nationwide Public Safety Broadband Network RFI additionally requested input to the below questions – CU-Boulder replied to those topics where we have sufficient expertise that would warrant advocating a position or expressing an opinion as follows:

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

CU-Response: It is absolutely critical – a Level-0 requirement. Open standards must be in place to guide manufacturers and vendors, conformance testing must be specified, and an independent compliance assessment entity must exist.

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

CU-Response: Functional commonality is a desirement, not necessarily a requirement. Specifying of functional commonality should not hamper a vendor's ability to provide alternative competitive solutions.

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

CU-Response: It is critical in the PSBN arena where the U.S. Government is utilizing commercial vendor infrastructure. The network environment must be multi-vendor to assure the U.S. Government of competitive service provisioning. Other lessons include: Open standards must be in place to guide manufacturers and vendors, conformance testing must be specified, and an independent compliance assessment entity must exist.

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

CU-Response: An open standards-based middleware should be utilized to protect the substantial investment in legacy hardware and to provide a transition path for future PSBN device hardware.

Should the goal 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?

CU-Response: We would advocate for a separate survivable core that works with the PSBN but is physically and logically separated. Possibly the government could manage the survivable core, or a non-profit NGO (Non governmental organization) could manage and operate the survivable core infrastructure.

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

CU-Response: We don't have the cellular market expertise to provide an opinion on this topic.

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?

CU-Response: DTN, middleware, DataVac.

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?

CU-Response: A government (NIST) review board coupled with an Industry/Academia review board.