



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

May 14, 2014

Ms. Charlotte Savercool
Committee on Energy and Commerce
United States House of Representatives
Washington, D.C. 20515

Dear Ms. Savercool:

Attached is the National Institute of Standards and Technology's (NIST) responses to the questions for the record from the November 21, 2013, hearing before the House Energy and Commerce Subcommittee on Communications and Technology on "*Oversight of FirstNet and the Advancement of Public Safety Wireless Communications*" in which the NIST Public Safety Communications Research (PSCR) Program Manager, Dereck Orr, testified.

If you have any questions, please contact me at (301) 975-3075.

Sincerely,


Kandy J. Hawk
Congressional and Legislative Affairs

Attached

The Honorable Greg Walden

- 1. FirstNet will remain a data only network until the 3GPP standards are developed for mission-critical voice over LTE. The Middle Class Tax Relief and Job Creation Act of 2012 directed the National Institute Standards and Technology (NIST) to, among other things, accelerate the development of “mission critical voice” and do so in consultation with FirstNet and the Public Safety Advisory Committee (PSAC). Please explain what NIST has done in consultation with the PSAC to advance the development of mission critical voice over LTE. Is NIST consulting with private industry in the development of these standards? If so, please explain.**

Answer:

Public Safety Communication Research (PSCR) staff from both the National Institute of Standards and Technology (NIST) and the Institute for Telecommunication Sciences (ITS) of the National Telecommunications and Information Administration (NTIA), have been participating in Long Term Evolution (LTE) standards development since November 2012 within the 3rd Generation Partnership Project (3GPP) which is responsible for the creation of LTE standards and specifications. These efforts have been focused on developing mission critical voice capabilities for public safety in the LTE standards. Specifically, the focus has been on developing standards for direct mode communications, efficient group communications, and push-to-talk communications. In addition, the National Public Safety Telecommunications Council’s (NPSTC) Broadband Working Group (BBWG), which develops public safety broadband communications requirements, has created two requirements documents for public safety broadband. The first was a Launch Requirements document that detailed public safety’s expectations for FirstNet to deliver at launch of the network, and the second was a Mission Critical Push-to-talk over LTE Requirements document that detailed public safety’s expectations for mission critical voice on the FirstNet network. PSCR staff was involved in the development of both of these documents, which were delivered to FirstNet’s Public Safety Advisory Committee (PSAC), who reviewed and modified the documents where necessary before delivering them to FirstNet for use. Both of these documents are being actively used by FirstNet in the development of RFI/RFP’s and in the development of standards pursuant to mission critical voice and data over LTE.

NIST works collaboratively with all 3GPP industry members within the standards process to develop consensus-based solutions. In addition, since 2010, the PSCR program, in partnership with the Department of Homeland Security (DHS) Office for Interoperability and Compatibility (OIC), deployed in the Boulder, CO, area a first-of-its-kind fourth generation (4G) Long Term Evolution (LTE) 700 MHz Public Safety Broadband Demonstration Network. This network was developed in collaboration with industry through Cooperative Research and Development Agreements (CRADAs) between NIST, NTIA, and over 75 individual industry partners to date. This public-private partnership has resulted in one of the most vendor-diverse 4G LTE networks in the world and is another example of NIST collaborating with industry to develop new technologies and standards for public safety.

2. Please estimate to the best of your knowledge when mission critical voice over LTE will be available to users of the FirstNet network.

Answer:

It is very difficult for the PSCR to forecast when a type of product may become available in the public safety marketplace, given that such a decision will be highly dependent on the independent business decisions made by multiple companies to develop and market such products, as well as public safety's acceptance that the new devices do in fact meet the criteria to be considered public safety mission critical voice compliant.

However, given the rapid advancement in the state of the standards due to significant work by organizations such as FirstNet, PSCR, the public safety community, and numerous industry partners, the PSCR's expectation is that within the next 18 to 24 months we might start seeing prototypes in our laboratories that display multiple capabilities associated with public safety mission critical voice (e.g., direct mode, group communications, and push-to-talk). This will allow us to start assessing, testing and reiterating on the standards to ensure these products meet public safety mission critical voice requirements at a future date.

3. Please describe how the Public Safety Communication Research (PSCR) Program is structured and funded. Please identify the expenditures of funds by PSCR by program or activity.

Answer:

The PSCR is a joint program within the Department of Commerce (DOC) between NIST and NTIA ITS headquartered at the DOC labs in Boulder, CO. The PSCR is comprised of approximately 40 staff and contractors from NIST and ITS and is managed overall by a NIST Program Manager and a ITS Deputy Program Manager. Over the last 15 years, the PSCR has used this partnership to leverage the scientific and engineering skills across both agencies to develop dynamic teams of experts to advance public safety communications technologies.

Funding for the PSCR primarily comes from external Federal sponsors. The longest standing program sponsor is DHS OIC within the Science and Technology Directorate. The PSCR has received expanded sponsorship from DHS Office of Emergency Communications (OEC) to provide research, testing, and standards support for OEC's Wireless Priority Services related activities. Additionally, PSCR is sponsored by the First Responder Network Authority (FirstNet) to advance public safety broadband communications standards, and is receiving additional funding in FY14 for research projects related to public safety broadband communications that PSCR is uniquely qualified to execute. The strong partnership among OIC, OEC, FirstNet, and the PSCR program is an excellent example within the Administration of multi-agency coordination and collaboration, and is something of which NIST and NTIA are very proud.

For FY14 the PSCR has currently available the following amounts by sponsor and activity (Note: A portion of these funds will be carried over into FY15 to fulfill period of performance):

NIST: \$1,000,000

Period of Performance: Funds expire September 30, 2014

Activity:

- Program Management and Stakeholder Outreach: \$650,000
- Future R&D Public Safety R&D Roadmap Development: \$240,000
- Other Objects (Equipment and Travel): \$110,000

DHS OIC: \$4,024,200

Period of Performance: Until September 30, 2015

Activity:

- Modeling and Simulation: \$950,000
 - Nationwide network planning
 - LTE Physical Layer Performance Characterization
 - Incident Scenario and Network Performance
 - Infrastructure Failure and Network Resiliency
 - Small Cell Deployments/In-building coverage
- Testing and Evaluation: \$2,175,000
 - Land Mobile Radio (LMR) to Public Safety Long Term Evolution (LTE) Interoperability
 - Public Safety Video Quality
 - 700 MHz LTE Demonstration Network
 - Project 25 (P25) Compliance Assessment Program (CAP)
 - Public Safety Audio Quality
- LMR and LTE converged device project for DHS Customs and Border Protection (CBP): \$424,200
- Requirements Gathering: \$68,000
 - Public Safety LTE Broadband Requirements
- Security: \$407,000
 - Identity Management
 - Mobile Applications

DHS OEC: \$3,963,000

Period of Performance: Funds expire September 30, 2014

OEC had engaged the PSCR program to support OEC in the development and implementation of Next Generation Network (NGN) Priority Services and to ensure that it is compatible with the Nationwide Public Safety Broadband Network (NPSBN).

Activity:

- Standards Development: \$1,000,000

- Develop an overall standards development approach for NS/EP efforts for the creation of priority services on commercial and private Long Term Evolution (LTE) broadband networks.
- Testing and Evaluation: \$950,000
 - Establish an overall test and evaluation testbed framework utilizing existing and/or new broadband equipment and on-site capabilities at the PSCR laboratories to develop, test, and/or verify NGN Priority Services approaches
- Modeling and Simulation: \$986,000
 - Develop and enhance modeling and simulation efforts related to the network performance and analysis of NGN Priority Services.
- Stakeholder Engagement and Practitioner Travel: \$1,027,000

FirstNet: \$5,595,400

Period of Performance: Funds expire April 30, 2015

Activity:

- Standards Development: \$2,015,400
 - Direct Mode capability
 - Efficient Group Communications
 - Mission Critical Push-to-talk
- Testing and Evaluation: \$1,540,000
 - Priority and Quality of Service validation
- Modeling and Simulation: \$1,040,000
 - Radio Access Network (RAN) modeling and simulation
 - Core modeling and simulation
- Other Objects (Equipment and Travel): \$1,000,000

4. Please describe the work performed by PSCR related to FirstNet's deployment of a nationwide public safety broadband network by project or activity. Please describe the status of this work. Please identify the amount of funds expended on this work by project or activity.

Answer:

The ITS side of PSCR has been funded since November 2012 to perform standards development work in 3GPP for FirstNet. Beginning in FY2014, that work is expanding to encompass additional tasks as outlined in the response to Question #3. Additional information related to the specifics of the three task areas are as follows:

- Standards: Participate in relevant commercial standards development organizations such as the 3rd Generation Partnership Project (3GPP), in consultation with FirstNet. Develop and submit technical standards recommendations to the appropriate FirstNet Board committees. These efforts

will build upon previous PSCR standards development activities. PSCR staff will serve as subject matter experts within relevant standards organizations, in consultation with FirstNet.

- \$2,015,400
- Testing and Evaluation: Establish an overall research and development test and evaluation testbed framework at the DOC Boulder laboratories. In consultation with FirstNet, NIST Office of Law Enforcement Standards (OLEs) staff within the PSCR will perform research and development testing related to existing vendor products, new cutting edge technologies, possible system architectures, and assessing the common implementation of commercial standards and key first responder features and report those research and development testing results to FirstNet.
 - \$1,540,000
- Modeling and Simulation: Provide modeling and simulation support to FirstNet technical staff related to a nationwide deployment as well as state and local network designs. This work will include RAN Modeling and Simulation and Core Modeling and Simulation.
 - \$1,040,000
- Equipment, Travel, and Training:
 - \$1,000,000

5. Given FirstNet's mission it can be assumed that the network will likely be a target of cyber attack? Has PSCR been involved in work to develop cybersecurity safeguards for the FirstNet network? If so, please describe.

Answer:

Cyber security has not been a primary focus of the PSCR in the past, however, through sponsorship from DHS OIC, the PSCR will be undertaking several specific research projects related to public safety security.

Based on the National Public Safety Telecommunications Council's (NPSTC) Public Safety High-Level Launch Requirements released in December 2012, the public safety community expressed their need for a Nationwide Public Safety Broadband Network (NPSBN) to provide capabilities to secure and control access to the network, applications, and data. Some of the security concerns reflected in the high-level launch requirements are (a) securing the network interfaces and data traversing the network, (b) managing the identities of users and devices to control access to the network functionality and data, and (c) protecting network functionality and data from mobile application weaknesses and vulnerabilities.

The 3rd Generation Partnership Project (3GPP), which establishes LTE standards, has specified optional capabilities to secure the network interfaces between mobile devices (UEs) and base

stations (eNodeBs) as well as base stations (eNodeBs) and the core network (EPCs). Since the network interface security capabilities are optional, it is unclear to what extent these capabilities have been implemented in LTE equipment and their ability to support standards based interoperability. In addition, the public safety community has indicated the need to leverage virtual private network (VPN) and mobile VPN (mVPN) technologies to enable secure tunnels between mobile devices and its provisioning organization's network, applications, and data. However, it is unclear the impact VPN technology will have on the performance of mobile devices and the network as well as their ability to support call prioritization. As part of upgrading the PSCR Broadband Demonstration Network, PSCR will work to ensure the LTE network equipment support the 3GPP capabilities to secure the network interfaces. Working with the vendor and public safety communities, PSCR will develop use cases to investigate the ability of LTE equipment to secure network interfaces and support standard based interoperability; and the impact VPN technology has on network performance and call prioritization. The use cases developed can then be used to create test cases for the PSCR Broadband Demonstration Network.

Identity management is a fundamental security requirement used to limit and control access to network functionality and data. The NPSTC high-level launch requirements have several requirements related to identity management, authorization, and access control. One significant public safety requirement is the ability to not only identify a device on the network but the ability to identify a specific user of the device since different users may use the device. There are several different identity management technologies for mobile devices that could be leveraged to support public safety's requirements. These technologies have different form factors with associated benefits and disadvantages. One form factor may work well for a given set of users while that same form factor may not be useful or practical for another set of users. Working with the public safety community, PSCR will document the various identity management technologies for mobile devices, their advantages and disadvantages, and potential applicability to the public safety community.

With the deployment of a public safety LTE network, the bandwidth made available to the public safety community will provide the opportunity for sharing information via advanced applications and services. However, applications provide the opportunity for software weaknesses and vulnerabilities to disrupt network operations and access to information improper authorization. There are several NPSTC requirements related to mitigation techniques to limit and control the malfeasance of vulnerable and/or malicious applications such as using malware/virus scanners, access control techniques, and application management. In addition to these mitigation techniques, application software weaknesses and vulnerabilities could be reduced by using software assurance techniques as part of an applications development lifecycle. PSCR will interact with the public safety, mobile app developer, and test tool communities to ensure public safety security concerns from software based weaknesses and vulnerabilities are included in software assurance tools. In addition, PSCR will develop test suites based on public safety security issues caused by software weaknesses that can be used to exercise mobile application testing tools.