Comment 7: Name Corrections for Certain Companies

[FR Doc. 2011–23278 Filed 9–9–11; 8:45 am]

BILLING CODE 3510–DS–P

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. Mr. Orr's e-mail address is *dereck.orr@nist.gov*.

SUPPLEMENTARY INFORMATION: The public safety community (law enforcement, fire, and emergency medical service) is experiencing a generational shift in technology that will revolutionize the way it communicates. Traditionally, emergency responders have used land mobile radio technology. This technology has limited data capabilities and suffers from a large installed base of thousands of stand-alone proprietary systems with non-contiguous spectrum assignments. As a result, public safety has long struggled with effective cross-agency/jurisdiction communications and lags far behind the commercial sector in data capability. Congressional legislation has made broadband spectrum that was cleared by the transition from analog to digital broadcast television (referred to as the Digital Television (DTV) Transition) available to public safety for broadband communications. The newly available spectrum will allow for a unified system operating on common spectrum bands, fostering nationwide roaming, interoperability, and access to broadband data. However, public safety has several unique requirements that are not currently reflected in broadband technology.

In August 2010, the U.S. Department of Justice Community Oriented Policing Services (COPS) office held the National Forum on Public Safety Broadband Needs. More than 20 public safety practitioners identified the following 15 operational requirements, each of which relate to at least four overarching themes (resiliency, availability and reliability, security, and affordability/commercial alignment):

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

(2) At a minimum, 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) When voice is converged for normal operations and in the event the infrastructure is compromised, public safety communications must remain stable and with clear voice communications;

- Infrastructure-less communications, with talk-around for the ability to talk one-to-one and one-to-many
- Optimal audio quality during adverse field conditions
- No latency on mission critical voice applications

(5) Geographic coverage that has no limitations within the footprint of the National Public Safety Broadband Network;

(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 information sources;

(12) Easy integration with other technologies;

(13) Automatic management and control of the network;

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

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

The COPS report is available at: *http://www.cops.usdoj.gov/files/RIC/Publications/e021111338-broadband-forum.pdf.*

Since then, the Obama Administration has announced its support for legislation that would create a not-for-profit Public Safety Broadband Corporation to oversee the deployment of a nationwide network that meets the needs of local, state, Tribal, and Federal public safety communities.[1] The Administration has also proposed a $3 billion WIN Fund to help drive innovation through research, experimentation, testbeds, and applied development. Of the $3 billion, $500 million will be devoted to research and development (R&D) for the new public safety broadband network.[2] The Public Safety Innovation Fund (PSIF), NIST's component of the proposed WIN Fund, helps spur the development of cutting-edge wireless technologies. NIST is working with industry, its Federal partners and public safety organizations to conduct R&D to support new standards, technologies and applications to advance public safety communications. Core components of this program include documenting public safety requirements and driving the adoption of those requirements into the appropriate standards; developing the capability for communications between currently deployed public safety narrowband systems and the future nationwide broadband network; and establishing a roadmap that seeks to capture and address public safety's needs beyond what can be provided by the current generation of broadband technology and driving technological progress in that direction. Through pre-competitive research, development, reference applications, and demonstration projects, NIST will accomplish these goals.

In pursuit of these goals, NIST seeks comments on the following possible features of the nationwide public safety broadband network. These more

[1] Comments of the National Telecommunications and Information Administration before the Federal Communications Commission in the matter of Service Rules for the 698–747, 747–762 and 777–792 Band (WT Docket No. 06–150); Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band (PS Docket No. 06–229); Amendment of Part 90 of the Commission's Rules (WP Docket No. 07–100). *http://www.ntia.doc.gov/filings/2011/NTIA_Public_Safety_Network_Comments_06102011.pdf.*

[2] President Obama Details Plan to Win the Future through Expanded Wireless Access. *http://www.whitehouse.gov/the-press-office/2011/02/10/president-obama-details-plan-win-future-through-expanded-wireless-access.*

technical features were identified by the NIST Visiting Committee on Advanced Technology with the input of public safety and their identified operational requirements. Among other things, NIST seeks to understand the extent to which these features and requirements can be satisfied through existing commercially available technology or though technology that could become available in the relative short-term, assuming appropriate research and development. Information obtained from this solicitation will be used to inform the potential use of grant funds to spur innovation in those areas not currently commercialized.

Feature List (organized around the four overarching themes noted above):

To ensure resiliency in an emergency:

• *Resiliency:* The ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements.[3]

• *Self-Organizing:* Self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.[4]

• *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.[5]

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

To ensure reliability and availability:

• *Prioritization:* The ability to prioritize network traffic based on assigned priority schemes.

• *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.[6]

To enable security:

• *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 entree into a broad set of systems and databases needed by public safety (*e.g.,* criminal history databases, medical records, public work records, *etc.*).

To ensure affordability/commercial alignment:

• *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.

• *Network sharing:* The shared use of infrastructure between commercial and public safety users.

• *Multi-Modal:* The ability of the network to support voice, video, data, and multimedia simultaneously.

• *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.

• *Power Awareness:* The ability of network/devices to control power functions.

• *Standardized Common Interfaces:* Protocols, Application Program Interfaces, application platforms, radio capabilities, etc. that allow for competitive provisioning.

• *Uniform, Universal Access:* The ability to access the network and data anywhere at any time through any device.

Request for Comments

For each feature listed above, NIST is requesting input on the following:

• Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

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

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

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

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

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

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

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

• 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?

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

• 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.[9] 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.

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

• 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?

• 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?

This request for information coincides with other work NIST is doing to support the nationwide public safety broadband network, including a demonstration network from the Public

[3] *http://publicsafety.fcc.gov/pshs/clearinghouse/core-concepts/resiliency.htm.*

[4] *http://www.wina.org/WireSol/Documents/Whitepaper%20-%20Self%20Organizing%20Networks%20for%20In-Plant%20Applications.pdf.*

[5] *http://en.wikipedia.org/wiki/Mesh_networking.*

[6] http://*technet.microsoft.com/en-us/library/cc757120(WS.10).aspx.*

[7] *http://en.wikipedia.org/wiki/Access_control_list.*

[8] *http://en.wikipedia.org/wiki/Scalability.*

[9] President's Council of Advisors on Science and Technology, Report to the President and Congress (Dec. 2010) (*http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf*), pp. 55–56.

Safety Communications Research program in Boulder, Colorado.[10]

Dated: September 6, 2011.

Willie E. May,

Associate Director for Laboratory Programs.

[FR Doc. 2011–23180 Filed 9–9–11; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XA681

Marine Mammals; Pinniped Removal Authority

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; request for comments.

SUMMARY: NMFS received an application under section 120 of the Marine Mammal Protection Act (MMPA) from the states of Idaho, Oregon and Washington (states) requesting authorization to intentionally take, by lethal methods, individually identifiable California sea lions (*Zalophus californianus*) that prey on Pacific salmon and steelhead (*Onchorhyncus spp.*) listed as threatened or endangered under the Endangered Species Act (ESA) in the Columbia River in Washington and Oregon. This authorization is requested as part of a larger effort to protect and recover listed salmonid stocks in the river. Pursuant to the MMPA, NMFS has determined that the application contains sufficient information to warrant convening a Pinniped-Fishery Interaction Task Force (Task Force), which will occur after the close of the public comment period. NMFS solicits comments on the application and other relevant information related to pinniped predation at Bonneville Dam.

DATES: Comments and information must be received by October 12, 2011.

ADDRESSES: You may submit comments, identified by NOAA–NMFS–2011–0216, by any of the following methods:

Electronic Submissions: Submit all electronic public comments via the Federal eRulemaking Portal *http://www.regulations.gov.*

Mail: Comments on the application should be addressed to: Assistant Regional Administrator, Protected Resources Division, NMFS, 1201 NE. Lloyd Blvd., Suite 1100, Portland, OR 97232.

Instructions: All comments received are a part of the public record and will generally be posted to *http://www.regulations.gov* without change. All Personal Identifying Information (for example, name, address, *etc.*) voluntarily submitted by the commenter may be publicly accessible. Do not submit Confidential Business Information or otherwise sensitive or protected information.

NMFS will accept anonymous comments (enter N/A in the required fields, if you wish to remain anonymous). You may submit attachments to electronic comments in Microsoft Word, Excel, or Adobe PDF file formats only.

FOR FURTHER INFORMATION CONTACT: Garth Griffin, (503) 231–2005 or Brent Norberg (206) 526–6550 or Shannon Bettridge, (301) 427–8402.

SUPPLEMENTARY INFORMATION:

Electronic Access

Further information is available via the Internet, including the states' application, background information on pinniped predation on listed salmonids, NMFS' past authorizations of lethal removal at Bonneville Dam, descriptions of nonlethal efforts to address the predation, NMFS' 2008 Final Environmental Assessment, and 2011 Supplemental Information Report to the 2008 Final Environmental Assessment. The Internet address is: *http://www.nwr.noaa.gov/Marine-Mammals/Seals-and-Sea-Lions/Sec-120-Authority.cfm*

Statutory Authority

Section 120 of the MMPA (16 U.S.C. 1361, *et seq.*) allows the Secretary of Commerce, acting through the Assistant Administrator for Fisheries (Assistant Administrator), NMFS, to authorize the intentional lethal taking of individually identifiable pinnipeds that are having a significant negative impact on the decline or recovery of salmonids that are listed as threatened or endangered under the ESA. The authorization applies only to pinnipeds that are not listed under the ESA, or designated as a depleted or strategic stock under the MMPA. Pursuant to section 120(b) and (c), a state may request authorization to lethally remove pinnipeds, and the Assistant Administrator is required to: (1) Review the application to determine whether the applicant has produced sufficient evidence to warrant establishing a Task Force to address the situation described in the application; (2) Establish the Task Force and publish a notice in the **Federal Register** requesting public comment on the application if sufficient evidence has been produced; (3) Consider any recommendations made by the Task Force in making a determination whether to approve or deny the application; and (4) If approved, immediately takes steps to implement the intentional lethal taking, which shall be performed by Federal or state agencies, or qualified individuals under contract to such agencies.

The MMPA requires the Task Force be composed of the following: (1) NMFS/NOAA staff, (2) scientists who are knowledgeable about the pinniped interaction, (3) representatives of affected conservation and fishing community organizations, (4) treaty Indian tribes, (5) the states, and (6) such other organizations as NMFS deems appropriate. The Task Force reviews the application, other background information, the factors contained in section 120(d), and public comments and, as required by section 120, recommends to NMFS whether to approve or deny the application. The Task Force is also required to submit with its recommendation a description of the specific pinniped individual or individuals; the proposed location, time, and method of such taking; criteria for evaluating the success of the action; the duration of the intentional lethal taking authority; and a suggestion for non-lethal alternatives, if available and practicable, including a recommended course of action.

Background

In December 2006, NMFS received an application co-signed by the Washington Department of Fish and Wildlife, the Oregon Department of Fish and Wildlife, and the Idaho Department of Fish and Game requesting authorization to intentionally take, by lethal methods, individually identifiable California sea lions in the Columbia River, which are having a significant negative impact on the recovery of threatened and endangered Pacific salmon and steelhead. After deeming the states' application complete, NMFS published a notice in the **Federal Register** seeking public comment on the application and also requested names of potential members of the Task Force (see 72 FR 4239, January 30, 2007). After the close of the public comment period, NMFS announced the formation of the Task Force, which consisted of 18 members (72 FR 44833, August 9, 2007). The notice also identified a list of questions that NMFS considered relevant to its section 120 decision-making process. The Task Force completed and submitted its report to NMFS on November 5, 2007. Of the 18

[10] *http://www.pscr.gov/projects/broadband/700mhz_demo_net/700mhz_ps_demo_net.php.*