National Forum on Public Safety Broadband Needs

August 23, 2010

SEARCH

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

This project was supported by a Cooperative Agreement 2010-CK-WX-K004 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, companies, products, or services should not be considered an endorsement by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

The Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the author nor the COPS Office can vouch for their current validity.

February 2011

Introduction

The U.S. Department of Justice Office of Community Oriented Policing Services (the COPS Office), along with the U.S. Department of Homeland Security and U.S. Department of Commerce, hosted the *National Forum on Public Safety Broadband Needs,* held in Washington, D.C., August 19–20, 2010. The forum was attended by 21 active public safety practitioners on behalf of 15 of the original 700MHz waiver applicants, and represented a cross-section of urban, state, rural, and tribal public safety practitioners (law enforcement, fire, and emergency medical services) from around the country.

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.

The participants also helped define public safety's meaning of terms such as "public safety broadband" and "emergency" in the context of public safety broadband.

From the officer on the street to command staff and beyond, public safety relies on immediate, secure, accurate, and quality information to make critical decisions on a daily basis. National broadband offers many benefits to public safety with robust and resilient information sharing, but only if done right and within a reasonable timeframe. *The National Forum on Public Safety Broadband Needs* provided a looked-for opportunity for discussion, consensus building, and actionable outcomes that will help shape the direction of national broadband for our nation's public safety community.

This forum offered a unique perspective from the line officers/first responders in the field who are well versed in the operational requirements of their respective agencies. While the forum included stakeholders and representatives of the associations/working groups already participating in the national broadband debate, the COPS Office brought in additional practitioners directly involved in day-to-day operations of public safety communications who had not previously been engaged in the discussion. The forum was not intended to discuss the technical elements of broadband; rather, the focus was on public safety's *operational* requirements for voice and information sharing that will ultimately drive the technical elements of the National Public Safety Broadband Network.

The following information represents the collaborative work of this public safety focus group and the consensus reached over the one and a half days of engaged and deliberate discussions.

Definitions

These definitions were developed by the state, local, and tribal forum participants through consensus and in the context of their understanding of broadband as it relates to the national discussion about broadband, the subset of public safety broadband, and the National Public Safety Broadband Network.

PUBLIC SAFETY BROADBAND IS…

A high-speed, large capacity, resilient, affordable, and open standards-based capability to share tactical, operational, and strategic public safety voice and information* in a seamless and secure mobile environment.

AN EMERGENCY IS…

Imminent and/or perceived threat to life and/or property that can escalate quickly with varying degrees of scale.

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.

Operational Requirements for the National Public Safety Broadband Network

The operational requirements below are overarching statements supported by examples to illustrate their intention and meaning. Neither the statements nor examples are intended to be all-inclusive.

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.
        i. Ruggedized
        ii. Water-resistant and/or waterproof
        iii. Longer battery life
        iv. Intrinsically safe
        v. 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

Broadband Forum Participant Roster

Todd Bianchi
Firefighter NREMT-P
District of Columbia Fire and EMS Department

Police Officer Robert Cordasco
Boston (MA) Police Department

Deputy Chief Charles Dowd
New York City (NY) Police Department

Captain John Gibson
Chesapeake (VA) Fire Department

Lieutenant Barbara Hawkins
Metropolitan (DC) Police Department

Robert Jones
Assistant Director of Communications
New York State Police

Major Eddie Levins
Commander, Administrative Service Bureau
Charlotte-Mecklenburg (NC) Police Department

Deputy Chief David E. Martinez
San Antonio (TX) Fire Department

Lieutenant Anthony Maziek
San Antonio (TX) Police Department

Deputy Chief Christopher Moore
San Jose (CA) Police Department

Officer James Parks
New Mexico State Police

Lieutenant Lee Rankin
Mesa (AZ) Police Department

Assistant Chief Dick Reed
Commander, Field Support Bureau
Seattle (WA) Police Department

Captain Christian Schulz
Executive Officer
Emergency Management Section
New Jersey State Police

Inspector Keith Spadaro
Communications Division
New York City (NY) Police Department

Lieutenant Greg Staylor
Chesapeake (VA) Police Department

Sergeant Clark Tompsett
New Mexico State Police

Chief Richard Van Boxtel
Chief of Police
Oneida (WI) Tribal Police

Stephen Weston
Firefighter/Paramedic
Regional Interoperable Communications System (RICS)
Los Angeles County (CA) Fire Department

Chief Darin White
Battalion Chief
Oakland (CA) Fire Department

Lieutenant Mark Wilkins
Los Angeles County (CA) Sheriff's Department

Broadband Forum Observers

David Buchanan
Deputy Director
COPS Office
U.S. Department of Justice

James Burch
Acting Director
Bureau of Justice Assistance
U.S. Department of Justice

Marisa Chun
Deputy Associate Attorney General
U.S. Department of Justice

Chris Essid
Director
Office of Emergency Communications
U.S. Department of Homeland Security

Telford E. Forgety, III; "Trey"
Presidential Management Fellow
National Telecommunications & Information Administration
U.S. Department of Commerce

Dale Hatfield
Adjunct professor at the University of Colorado and Executive Director of the school's Silicon Flatirons Center

Taylor Heard
Counselor
Cyber Security and Communications
U.S. Department of Homeland Security

Joseph Heaps
National Institute of Justice
Information and Sensor Technologies Division
U.S. Department of Justice

John Markovic
Senior Social Science Analyst
COPS Office
U.S. Department of Justice

Bernard Melekian
Director
COPS Office
U.S. Department of Justice

Dereck Orr
Program Manager
Office of Law Enforcement Standards
National Institute of Standards & Technology
U.S. Department of Commerce

Gregory Schaffer
Assistant Secretary
Cyber Security and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Philip Weiser
Senior Advisor to the National Economic Council Director for Technology, Innovation, and Competition Policy

SEARCH Staff

Ronald P. Hawley
Executive Director

Kelly J. Harbitter
Deputy Executive Director
Programs Division

Doug Onhaizer
Director
Public Safety Programs

Nina K. Byrom
Administrative Assistant
Public Safety Programs

Ron Haraseth
Public Safety Technology Specialist
Public Safety Programs

Robert E. Nibarger
Public Safety Technology Specialist
Public Safety Programs

About COPS

The Office of Community Oriented Policing Services (the COPS Office) is the component of the U.S. Department of Justice responsible for advancing the practice of community policing by the nation's state, local, and tribal law enforcement agencies through information and grant resources. The community policing philosophy promotes organizational strategies that support the systematic use of partnerships and problem-solving techniques to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime. In its simplest form, community policing is about ***building relationships and solving problems***.

The COPS Office awards grants to state, local, and tribal law enforcement agencies to hire and train community policing professionals, acquire and deploy cutting-edge crime-fighting technologies, and develop and test innovative policing strategies. The COPS Office funding also provides training and technical assistance to community members and local government leaders and all levels of law enforcement.

Since 1994, the COPS Office has invested more than $16 billion to add community policing officers to the nation's streets, enhance crime fighting technology, support crime prevention initiatives, and provide training and technical assistance to help advance community policing. More than 500,000 law enforcement personnel, community members, and government leaders have been trained through COPS Office-funded training organizations.

The COPS Office has produced more than 1,000 information products—and distributed more than 2 million publications—including Problem Oriented Policing Guides, Grant Owners Manuals, fact sheets, best practices, and curricula. And in 2010, the COPS Office participated in 45 law enforcement and public-safety conferences in 25 states in order to maximize the exposure and distribution of these knowledge products. More than 500 of those products, along with other products covering a wide area of community policing topics—from school and campus safety to gang violence—are currently available, at no cost, through its online Resource Information Center at **www.cops.usdoj.gov**. More than 2 million copies have been downloaded in FY2010 alone. The easy to navigate and up to date website is also the grant application portal, providing access to online application forms.

Additional information regarding the COPS Office can be found at **www.cops.usdoj.gov**.

U.S. Department of Justice
Office of Community Oriented Policing Services
Two Constitution Square
145 N Street, N.E.
Washington, DC 20530

To obtain details on COPS programs, call the
COPS Office Response Center at 800.421.6770.

Visit COPS Online at www.cops.usdoj.gov

e021111338

February 2011