U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HEARING CHARTER

Interoperability in Public Safety Communications Equipment

Thursday, May 27, 2010
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

I. Purpose

Communication among first responders is essential in emergency response. Recent disasters, including 9/11 and the 1999 Columbine High School shooting, have illustrated the communication problems that can occur when multiple agencies respond to a disaster. Compatible technology is critical to enabling interoperability, or the ability of first responders to communicate with their counterparts from other agencies and jurisdictions. For two decades, the public safety community, private industry, and the federal government have been working on technical standards that will ensure that digital land mobile radio (LMR) systems from different vendors are interoperable. The purpose of this hearing is to discuss the status of these standards and the interoperability capabilities of public safety LMR equipment.

II. Witnesses

- **Dr. David Boyd**, Director, Command, Control & Interoperability, Science and Technology Directorate, Department of Homeland Security
- **Mr. Dereck Orr**, Program Manager, Public Safety Communications Systems, National Institute of Standards and Technology
- **Dr. Ernest L Hofmeister**, Senior Scientist, Harris Corporation
- **Mr. John Muench**, Director of Business Development, Motorola Inc.
- **Chief Jeffrey D. Johnson**, President, International Association of Fire Chiefs, and Chief, Tualatin Valley Fire and Rescue, Aloha, Oregon

III. Brief Overview

The public safety community has long recognized the challenge of providing for interoperable communications. Enabling first responders from different agencies and jurisdictions to communicate requires not only cooperation and planning, but also compatible technology. However, without common standards, there is no assurance that a manufacturer's proprietary systems will interoperate with its competitors' systems.

Since 1989, representatives from public safety, industry, and the government have been working together to develop common standards (known as the "P25" standards). The purpose of these standards is not only to ensure interoperability, but also to promote market competition, spectrum efficiency, and an easy transition from analog to digital radio systems.

Much progress has been made on these standards since 1989 and P25 radios and radio systems are now available. However, not all of the standards originally called for have been completed. As more public safety agencies make significant investments in radio systems, it is important to assess the status of the process and understand its impact on public safety.

In addition to the development of standards, assessing the compliance of P25 radios with the standards is critical for ensuring the investment made by governmental agencies will meet the expectations of the P25 process. Currently, there is no formal mechanism within the existing P25 process for validating that products claiming P25 compliance are in fact built correctly to the standards. The Department of Homeland Security (DHS) Compliance Assessment Program (CAP), a voluntary testing program, provides an alternative verification mechanism and is therefore an important tool for public safety in making equipment procurement decisions. However, the CAP currently does not require all of the testing that was originally envisioned.

IV. Background

Lack of Interoperability The lack of communications interoperability has posed significant challenges in the response to large-scale disasters, such as the 1995 Oklahoma City Bombing, the 2001 attack on the World Trade Center in New York City, and Hurricane Katrina in 2005. At the scene of the Oklahoma City bombing, fragmented communication frequencies and conflicting standards prevented police and fire agencies from communicating with the National Guard, Federal Emergency Management Agency, and other federal agencies. Lack of interoperability contributed to the chaos and tragedy of 9/11 when some 200 firefighter did not receive a message broadcast on NYPD radio channels that the collapse of the first tower was imminent. And, in the days immediately following Hurricane Katrina, local and federal agencies could not talk to one another. For example, first responders in helicopters were unable to communicate with crews patrolling in boats, hampering rescue efforts. Even the response to the Columbine High School shooting was hindered by a lack of interoperable equipment. Nearly 1,000 first responders from different agencies arrived on the scene but the lack of interoperability prevented them from being able to adequately assess the situation and the threat level, slowing the response. In these situations, first responders had to use message runners, an inefficient practice that limits the flow of information to incident commanders.[1]

[1] Tristan Weir, *Federal Policy Toward Emergency Responder Interoperability: A Path Forward*. Thesis submitted for a Masters of Science in Technology Policy from the Massachusetts Institute of Technology, 2006.

Enabling interoperability requires major planning and coordination among the agencies and jurisdictions that may need to work together when responding to a disaster. However, as the examples above illustrate, incompatible radio systems significantly hamper interoperability. Technology-based causes of interoperability include proprietary designs or unique configurations among different radio systems that operate in different frequencies of the radio spectrum. First responder agencies have used a variety of ad-hoc solutions to enable interoperability, such as swapping radios or creating mutual aid channels, but such solutions are less efficient than systems designed to interoperate.

Project-25 The process of developing open standards for digital public safety radios began in 1989, when the Association of Public-Safety Communications Officials (APCO) and the National Association of State Telecommunications Directors (NASTD), with the involvement of the Department of Justice (DOJ) and other federal agencies, launched Project-25 (P25). The developers initiated P25 with the goals of having a user-defined and user-driven standards process that would allow for interoperability, multi-vendor procurement of equipment, an easy transition from legacy analog equipment to digital equipment, and greater spectrum efficiency.

The involvement of the user community makes P25 a unique technical standards development process. The Telecommunications Industry Association (TIA), which is a standards development organization accredited by the American National Standards Institute (ANSI), write and maintain the technical standards documents. The public safety community interacts with TIA's technical standards process through a Steering Committee. Aided by a User Needs Subcommittee, the Steering Committee develops the Statement of User Requirements on which the standards are based. Memoranda of Understanding govern the interaction between TIA's standards development committees and the Steering Committee. This interaction is further facilitated by a working committee between the two groups.[2]

Public safety LMR systems include fixed infrastructure, such as towers and base stations, and portable units, such as handheld and car-mounted radios. P25 seeks to provide for standardization of eight interfaces where components of the LMR systems must communicate with each other.[3] The first set of standards developed focused on the Common-Air Interface (CAI), which defines the communication protocols between radio transmitters and receivers. This standard is intended to ensure that a portable radio from one manufacturer can communicate with a portable radio from another manufacturer. It is crucial for overall interoperability between two different systems. Other standards suites needed for interoperability cover the interfaces between the larger infrastructure components. These include:[4]

[2] The APCO 25/34 Interface Committee (APIC), a joint subcommittee of the Steering Committee and the TIA Private Radio Section.
[3] http://www.pscr.gov/outreach/p25dsr/menu_top/p25_interfaces.php
[4] *Project 25: The Quest for Interoperable Radios*, Issue Brief from the COPS Interoperable Communications Technology Program, Dan Hawkins, May 2007.

- The Console Subsystem Interface (CSI), which defines how radio frequency components of the system and console (such as the equipment used by dispatchers) connect with one another.
- The Fixed Station Interface (FSI), which defines how components of the radio system that are fixed in place (such as base stations) connect with other components of the system.
- The Inter-RF subsystem Interface (ISSI), which defines how different radio networks should connect with one another.

Although the P25 process began in 1989, the entire suite of standards for all eight interfaces is not yet complete. According to a 2007 Government Accountability Office (GAO) report,[5] despite spending over $2 billion from 2003 to 2005 on interoperability, many states were far from achieving that goal. GAO identified the slow rate of P25 standards development as among the myriad factors hindering faster adoption of interoperable public safety communications systems. The report noted that the P25 standards committees took four years (from 1989 to 1993) to develop the CAI, but that the committees developed no additional standards between 1993 and 2005 that could be used by manufactures for additional elements of a P25 compliant system.

Although GAO did find that "significant progress" was made in defining the three other interfaces most critical to interoperability after 2005, they cited concerns from participating National Institute of Standards and Technology (NIST) researchers that these standards were still incomplete, allowing manufacturers to develop products based on inconsistent interpretations. Tests conducted between 2003 and 2006 showed that these inconsistent interpretations caused P25 radios to fail aspects of interoperability tests.

The 2007 GAO report further cited concerns that the lack of compliance testing had limited the impact of the standards process for digital LMR systems. Developers include compliance tests within standards documents to provide a mechanism to validate whether a product is actually built to the standard and minimize issues that arise with inconsistent interpretations of the standard by different manufacturers. Without this testing, there is no way to validate that a product labeled "P25 compliant" will perform as intended.

In response to GAO's 2007 assessment that work on P25 had slowed after the CAI, TIA asserted that 114 standards and documents were in fact published between 1993 and 2005 and that manufacturers themselves had initiated compliance testing to ensure the interoperability of their products.[6] However, according to the Public Safety Communications Research (PSCR) program,[7] standardization for all eight of the P25

[5] *First Responders—Much Work Remains to Improve Communications Interoperability*. GAO-07-301, April 2007.

[6] http://www.tiaonline.org/gov_affairs/press_publications/documents/TIAResponsetoGAOReportonP25.pdf

[7] The PSCR program is housed in Boulder and is a joint effort between the National Institute of Standards and Technology/Office of Law Enforcement Standards (NIST/OLES) and the National Telecommunications and Information Administration/Institute for Telecommunication Sciences (NTIA/ITS). http://www.pscr.gov/projects/lmr/p25_stds_dev/p25_stds_dev.php.

standards remains incomplete. According to the PSCR program's *Project 25 Documents and Standards Reference* for May 2010: "For most cases, a P25 interface, service, or equipment standard is not complete until all documents that provide the Overview, the Protocol Specifications, the Protocol Conformance Test Procedures, the Performance Measurements Methods, the Performance Recommendations, and the Interoperability Test Procedures are published or are approved for publication by the appropriate [TIA] committee." Although much progress has been made, only the ISSI has been fully completed.

Involvement by the Federal Government Over the past 15 years, multiple federal agencies have addressed the interoperability issue, from the DOJ to the Federal Communications Commission (FCC). The current lead within the federal government is the Department of Homeland Security (DHS) SAFECOM program. SAFECOM provides technical research and development through the DHS Science and Technology Directorate and practitioner guidance and coordination through the Office of Emergency Communication.

Although federal agencies have been involved with P25 since it began, the 2004 *Intelligence Reform and Terrorism Prevention Act* (P.L. 108-458) specifically directed the Secretary of Homeland Security to establish a program to enhance the interoperability of public safety communications. In addition to facilitating planning and coordination among all levels of government, the legislation directed the Department of Homeland Security to work—in consultation with NIST, the private sector, and others—to "accelerate the development of national voluntary consensus standards for public safety interoperable communications."

Compliance Assessment Program (CAP) As noted above, no formal mechanism exists in the P25 process to validate that the radio equipment meets the standards. In the report accompanying the FY2006 *Department of Homeland Security Appropriations Act* (H. Rept. 109-241), Congress directed DHS to work with NIST and the DOJ on a P25 Conformity Assessment Program. The resulting DHS Compliance Assessment Program (CAP), which certifies testing laboratories and specifies which tests must be conducted, is a voluntary process for P25 equipment suppliers to show that their equipment meets." P25 standards for "performance, conformance, and interoperability." However, conformance assessment testing is not currently required, nor do CAP requirements exist for all eight interfaces.

The SAFECOM *Recommended Guidance for Federal Grant Programs* requires that grant applicants using DHS funds to purchase P25 equipment must obtain Supplier's Declaration of Compliance (SDoC) documents and Summary Test Reports (STR) when they purchase the equipment. DHS also provides a website (www.rkb.us) where manufacturers can post these documents.

Conformity assessment tests whether a manufacturer has interpreted and implemented a standard correctly. It is more rigorous than interoperability and performance testing and is arguably the best mechanism for ensuring that manufacturers are interpreting the

standards consistently and for ensuring that all standardized functions on the radio will interoperate. Finally, conformity assessment testing is considered important for ensuring the backwards compatibility of new technology that must be connected to legacy systems, sometime as many as 20 years old.

Additional Issues with P25 In addition to the concerns outlined above, GAO's 2007 assessment of interoperability identified two other issues preventing more widespread adoption of P25 equipment: (1) the lack of information and expertise among state and local agencies in buying equipment to meet their needs, and (2) the increased cost of P25 systems over conventional radio systems.

Digital radios are complex and manufacturers offer many different features and levels of functionality. GAO noted that agencies lacked comparative information about product functionality and typical first responder requirements. In addition, P25 radio units can cost more than 2- to 3-times the cost of conventional analog radios suitable for first responder use. Building an entire P25 LMR system, which is critical for interoperability, is also a major cost for municipalities.

700 MHZ and Public Safety Broadband Network The P25 standards cover interoperability for voice communications over digital LMR systems. With the availability of broadband, many public safety agencies are integrating data functions into their operations. Since there is no dedicated public safety broadband network, public safety agencies must use commercial wireless providers. A public safety broadband network is part of ongoing discussions on the use of the newly-available portions of the 700 MHz band. Public safety officials see the 700 band as a resource for extra voice capacity, broadband, and Voice-IP back-up systems. Many would like to see a public/private partnership build a network that would allow public safety priority access during an emergency but be available for commercial users during normal operation.

While public safety demand for spectrum is generally less than network capacity in normal operations, demand can often exceed capacity during a crisis. A public/private network would potentially allow for a more efficient use of resources, but commercial providers have been hesitant to commit to the extra requirements and hardening a public safety network requires. For example, public safety networks must be available in remote locations and the infrastructure must be able to withstand disasters, like hurricanes or earthquakes. The inability to solve these challenges contributed to the failure of the recent FCC auction of spectrum designated for a public safety/commercial carrier partnership (the "D-Block") to meet the reserve price.

Debate is ongoing on how to govern, finance, and build a network to provide greater spectrum resources to public safety. However, the National Public Safety Telecommunications Council, DHS, and NIST have developed a public safety Broadband Network Statement of Requirements document to offer guidance to the FCC, which has stated that a 700 Mhz public safety broadband network must be interoperable, but has not issued regulations on how such interoperability would be achieved. In addition APCO is identifying gaps in standards to ensure that the network will support interoperability and

roaming. Standards are particularly important if the national public safety broadband system is eventually built out as a system of networks.

Finally, the move toward broadband could pose a challenge as public safety agencies move to comply with FCC narrow-banding requirements. In 2004, the FCC mandated that by 2013, all public safety agencies needed to transmit using 12.5 kHz-wide channels, rather than using 25 kHz-wide channels. It has been further proposed that, by 2018, public safety will migrate to 6.25 kHz-wide channels and the P25 standards process is already in the process of developing standards for 6.25 kHz. As the name implies, though, data-rich broadband communication requires wider channels. Thus, within the public safety portion of the 700 Mhz band, systems will have to enable both broadband and narrowband transmissions.

V. Issues and Concerns

Status of Standards Project 25 began in 1989. Although the standards developers have made much progress since that time and P25 systems are now being fielded around the country, the complete suite of standards has not yet been completed. Continued advances in technology will mean continued updates and revisions for the P25 standards. However, as public safety organizations implement P25 systems, it is important to gain insight into how the status of the standards development process will affect their current operations and future procurements.

Compliance Assessment Program Radios are a lifeline for first responders. Ensuring that they work as intended is critical for the safety of these individuals and the lives and property they protect. It is also critical in ensuring that the significant amount of public money used to procure these systems is well spent and improves the communication capabilities of public safety agencies. The DHS CAP may provide the public safety community with the assurance that products sold as P25 compliant meet all of the requirements of the standards. Potentially, too, it may identify areas where the standard has not been uniformly implemented. While it is important to balance the time and expense incurred by manufacturers in performing compliance testing with the benefit to the public safety community, it is also essential that there is a trusted process available to ensure that P25 equipment is interoperable and meets the other requirements of the standards.

Future Issues P25 is unique in bringing the user community and industry together in the standards development process. Such cooperation in the standards process is important as public safety increases its use of broadband and other technologies.