Statement for the Record

Dr. David Boyd
Director; Command, Control and Interoperability Division
Science and Technology Directorate
Department of Homeland Security

Before the U.S. House
Committee on Administration
Subcommittee on Capitol Security

June 18, 2008

Introduction

Good afternoon Chairman Capuano, Ranking Member Lungren, and Members of the Subcommittee. Thank you for inviting me to speak to you today.

The Science and Technology Directorate's Command, Control and Interoperability Division (CID), within the Department of Homeland Security (DHS), uses a practitioner-driven approach to create and deploy information resources that enable seamless and secure interactions among homeland security stakeholders. Our goal is to ensure that stakeholders have comprehensive, real-time, and relevant information to protect the Nation.

As the members of this Subcommittee are well aware, the ability to communicate is essential to the success of any emergency response operation. Emergency responders need to share vital data and voice information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. A key mission of DHS is to strengthen interoperability by developing tools, such as reports and guidelines; best practices; and methodologies that emergency response agencies can use immediately. We are also developing both voice and data messaging standards, and testing communications equipment to those standards. But the key to a successful solution to improve interoperable communications requires a focus on user needs and requirements, so we rely on both practitioners and policy makers across disciplines, jurisdictions, and levels of government to ensure that our work is aligned with responders' needs.

We believe our focus on the practitioner level has done much to improve interoperability since the attacks of 2001.

- In 2004, the Office for Interoperability and Compatibility (OIC) developed the Interoperability Continuum to help policy makers understand what it takes to achieve interoperability: effective and collaborative governance, well designed standard operating procedures, well implemented technology, meaningful training and exercises, and the integration of all of these into day-to-day operations.
- In 2006, we conducted the National Interoperability Baseline Survey which revealed that approximately two-thirds of emergency response agencies use interoperability to some degree in their operations.
- In 2007, each of the major urban/metropolitan areas developed a Tactical Interoperable Communications Plan.
- Earlier this year, all 56 states and territories developed Statewide Communications Interoperability Plans.
- Later this year, the DHS Office of Emergency Communications will release the first *National Emergency Communications Plan*, which is informed by national principles developed by practitioners at every level of government.
- Later this year, we will pilot a multi-band radio which is capable of operating across different radio frequencies, across different modes—including both digital and analog—and with radios developed by different manufacturers.

System of Systems Approach

With emergency response practitioner input, we developed a core strategy for improving interoperability for the Nation's emergency response community which is focused on promoting a "system of systems" approach using standards-based communications equipment. This approach gives emergency response agencies the flexibility to select equipment that best meets their unique technical requirements and budget constraints; it also allows systems owned and operated by different emergency response agencies that may be developed by different manufacturers to communicate. The long-term strategy aims at building a system of systems so that separate agencies can join together using interface standards and a set of compatible procedures and training without having to discard huge investments in existing infrastructure. Ultimately, emergency responders operating on a system of systems will be able to respond to an incident anywhere in the Nation, using their own equipment, on any communications system, and on dedicated public safety spectrum as needed and authorized. We are working on identifying solutions that advance the emergency response community toward a reliable system of systems—one that is not dependent on any single technology but instead allows for maximum flexibility within and among numerous technologies.

Procuring a New System

The vast majority of vendors want to manufacture and sell effective products that allow emergency responders to better communicate. But often times, emergency response agencies lack the technical personnel required. As a consequence, we have focused on building tools to help agencies effectively communicate their requirements to the manufacturers and we have worked directly with many agencies to help them make wise communications systems purchases. This experience has highlighted for us several issues that need to be considered by any emergency response agency considering the procurement of a new system:

Requirements

First, the agency has to comprehensively identify and describe its system and operational requirements. Agencies must be able to articulate exactly what they need, both in the request for proposals and in the contract so responding vendors know what they must be able to do, and so the agency knows what it must demand from its new system. This will be especially important for any new system in the Capitol, because yours is an unusual environment. The nature of the Capitol campus and its construction makes communications within and between buildings challenging; communications in tunnels and subways require especially robust designs; and because the National Capitol Region is one of the most RF intensive places on Earth—that is, it has different transmitters in operation all the time—interference, both direct and indirect, are unusually severe. To help local agencies identify requirements, practitioners worked with us to develop a national Statement of Requirements (SoR) for Public Safety Wireless Communications and Interoperability which provides a comprehensive set of emergency response communications requirements that can be used as a model for the development of specific agency requirements.

Digital vs. Analog

Some vendors have suggested that digital systems are always superior to analog systems and that digital systems are essentially immune to interference. While we are moving into a digital world because it offers a number of significant advantages, digital radios do not necessarily solve all the problems faced by emergency responders. For example, in some situations, digital systems can be more susceptible to interference than analog systems, and interference can have more severe consequences for digital signals. While interference in an analog radio system may result in dropping words or parts of words, interference in a digital system can block communications entirely. For example, firefighters report that background noise, such as sirens, helicopters, breathing apparatus, or alarms, can cause unintelligible audio in portable, two-way digital radios. We are working with the International Association of Fire Chiefs, the National Institute of Standards and Technology, manufacturers, and fire service leaders to identify the causes of and potential solutions to this critical problem. Digital systems are the future of communications, but they are not a panacea. Effective requirements gathering and sound systems engineering principles remain the most fundamental elements of any successful system development.

Testing and Acceptance

In addition to firm and detailed requirements, a thorough testing, evaluation, and acceptance process must be established before a contract is awarded and should be carefully spelled out in the contract. It is essential that agencies and vendors clearly understand the expectations for the new system as well as potential obstacles and that robust, demanding testing be conducted—not in a laboratory or factory, but in actual operational use—to ensure the new equipment really satisfies requirements and is fully operational. Testing of this kind should include individual component testing and end-to-end system testing to ensure all portions of the system work together and meet the specified requirements. When new systems fail in the field, it is almost always because they were accepted from the vendor without adequate, demanding testing.

Proven Technology

When possible, agencies should purchase a proven technology that has been fully tested and piloted by the vendor in other emergency response environments that are as much like the environment in which the purchasing agency will be using the equipment as possible. They should also purchase technology early enough in the technology lifecycle so that it meets current interoperable communications standards; the vendor can also include in the contract an agreement that the system will continue to be supported for at least 10-15 years after acceptance.

Beyond Voice

Although we usually think of voice communications when discussing radio interoperability, agencies should also consider broader requirements and design the system so it can support other critical functions, such as the transmission of critical text, imagery, and other information.

Lifecycle Strategy

Finally, agencies should develop a strategy that will allow for updates to the system. A lifecycle approach to the design of the system can help ensure the system can be gracefully updated as enhanced technologies and capabilities become available. Such a strategy will allow the agency to extend the life of the system by making more gradual infrastructure investments over time instead of being forced to make a wholesale replacement once the system is so old it verges on collapse.

Conclusion

Interoperability is not solely a technology problem that can be solved with just the "right" equipment or the "right" communications system. All of the critical factors for a successful interoperability solution—governance, standard operating procedures, training and exercises, and integration of the system into daily operations—*as well as* technology—must be addressed.

I appreciate the opportunity to testify before you today. I would be pleased to answer any questions you may have.