

Statement for the Record

David G. Boyd, Ph.D.

Director, SAFECOM Program Office

Science and Technology Directorate

Department of Homeland Security

Before the U.S. House of Representatives

Committee on Government Reform

Subcommittee on National Security, Emerging Threats, and International
Relations

July 20, 2004

Table of Contents

Introduction.....	3
Portfolio Areas	4
Office Implementation	5
Players: Owners, Partners, and Stakeholders.....	6
Principles for Achieving Interoperability	7
The Communications Portfolio - SAFECOM.....	8
SAFECOM Achievements To Date.....	10
SAFECOM On Track to Achieve Critical Milestones in 2004, including (but not limited to):.....	11
Conclusion	13

Introduction

Good morning and thank you, Mr. Chairman and Members of the Subcommittee for the invitation to speak to you today. I appreciate your interest in The Department of Homeland Security's interoperability efforts and am grateful for this opportunity to address the important issue of public safety interoperability and compatibility before you. Today's testimony will focus on the relationship the Department of Homeland Security (DHS) has with the Federal Communications Commission (FCC), and State and local agencies interested in executing common interoperability standards.

Public Safety Background

As Secretary Ridge stated on February 24, 2004,

The ability for our Nation's first responders to communicate with each other as well as share equipment in times of crisis is a critical issue facing our Nation. Solving this challenge is a long-standing and complex problem. There are, however, some immediate steps the department can take this year to address the ... communications and equipment needs of first responders and make substantial progress toward achieving the penultimate communications solution.

Communications interoperability is the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, as authorized. The Nation is heavily invested in an existing infrastructure that is largely incompatible. Currently, efforts within the Federal Government to address the interoperability problem are being coordinated with Federal, State and local practitioners. However, there remain many challenges, both technical and cultural, facing the improvement of public safety communications and interoperability.

Whether fighting a fire or responding to a terrorist attack, efficient and effective emergency response requires coordination, communication, and the sharing of vital information and equipment among numerous public safety and security agencies. As the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* makes clear, "systems supporting emergency response personnel, however, have been specifically developed and implemented with respect to the unique needs of each agency. Such specification complicates interoperability, thereby hindering the ability of various first responder organizations to communicate and coordinate resources during crisis situations." DHS believes this issue is so important that it has identified interoperability of communications and equipment as the number two priority for the Department's second year. We seek to ensure the interoperability of critical emergency response systems or products by making it possible for them to work with other systems or products without special effort on the part of the user.

The Department also has developed intradepartmental program offices to address the needs identified by emergency response providers¹ and to respond to the problems identified in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The National Strategy for Homeland Security also identifies “ensuring seamless communications among all responders a DHS priority. One of the new interdepartmental offices is a program office charged with significantly improving the coordination and validation of the Department’s interoperability programs, thus allowing firefighters, police officers and other emergency personnel to better communicate and share equipment with each other during a major disaster.

Since its beginning, the Department has been involved with the issue of wireless interoperability through project SAFECOM (Wireless Public SAFETY Interoperable COMMUNICATIONS) As a public safety practitioner driven program, SAFECOM, housed within the Department, has been the Federal Government’s central point in coordinating Federal wireless investments and activities and partner with State, local, and Tribal governments to improve the interoperability of our Nation’s wireless communications.

Secretary Ridge has now specifically tasked the Science and Technology (S&T) Directorate within DHS, in coordination with other DHS programs, to lead the planning and implementation of an office of interoperability that will address the larger issues of interoperability and compatibility, including wireless communications. By coordinating and leveraging the vast range of interoperability programs and related efforts spread across the Federal Government, this office, currently titled the “Office of Interoperability and Compatibility” (OIC), will reduce unnecessary duplication in programs and spending and ensure consistency across federal activities related to research and development, testing and evaluation (RDT&E), standards, technical assistance, training, and grant funding related to interoperability. This new program office will also encompass the SAFECOM office, which will continue as a key national initiative within the communications programs of OIC, in the Department’s efforts to address the larger issue of interoperability.

Portfolio Areas

Within OIC, DHS is creating a series of portfolios to address critical issues related to the emergency response provider and homeland security communities. Initial priority portfolio areas the office will be addressing, in coordination with other departmental offices such as the DHS Office for Domestic Preparedness (ODP), include:

- Communications (through the SAFECOM Program Office);
- Equipment;
- Training; and

¹ As defined in the Homeland Security Act of 2002, Section 2(6), “The term ‘emergency response providers’ includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities.” 6 U.S.C. 101(6)

- Others as required.

The OIC currently is identifying the necessary Federal stakeholders and will utilize these stakeholders to assess and finalize the portfolio areas. Through this process, the OIC will identify existing initiatives as well as the most appropriate short-term deliverables.

Office Implementation

The OIC is being modeled after the SAFECOM Program, which represents a successful model for how to address highly sophisticated technical and policy issues associated with public safety communications and interoperability. Leveraging the work that the SAFECOM Program has already undertaken, the OIC will look to replicate relevant elements of the SAFECOM process and to build on SAFECOM's achievements in bolstering public safety communications.

The new OIC will employ a systems engineering or lifecycle approach to identifying, defining, and developing action plans in each portfolio area. This lifecycle approach is both iterative and collaborative. It emphasizes the need to create a common set of standards, policies, and procedures that encourage backwards compatibility of new solutions which will drive the migration of systems towards advanced, interoperable equipment and processes in the future. Common components of this lifecycle approach include:

- Validation of needs assessments (consistent with Homeland Security Presidential Directive-8, which lays out the National Preparedness Goal, as appropriate);
- Development, with the user community, of a comprehensive statement of requirements for each portfolio;
- Completion of baselines to provide starting points for each portfolio;
- A robust research and development program for new capabilities;
- A robust standards program to identify and adopt existing, effective standards for public safety equipment and to support the development of essential new standards when none exist.
- Testing and evaluation of existing technologies;
- Development of common standards for training and technical assistance;
- Development of appropriate grants/funding guidance; and
- Development of policy and legal reference materials or recommendations relevant to each portfolio.



Within the OIC, we are following the successful SAFECOM model by creating action plans for each of these areas, and for others identified as the portfolios are developed. Each of these action plans will be developed through a collaborative process that brings together the relevant stakeholders to provide clear direction on a path forward. The process to develop action plans will involve:

- Assessment of the government agencies involved in each portfolio;
- Identification of the relevant stakeholders at the Federal, State and local levels;
- A stakeholder working session to define the issues, assess user needs, and create a detailed vision of the “end state” for each portfolio; and
- A governance structure that ensures ongoing participation on the part of key stakeholders at the Federal, State and local levels.

Through this end-user input, the new OIC will produce a strategy and action plan to address the interoperability and compatibility needs in each of these portfolios.

The OIC structure will be an organizational reflection of the lifecycle process it is designed to manage and support. The main purpose of the OIC will be to provide common standards of practice, protocol, planning, and evaluation across the broadest spectrum of interoperability activities and to facilitate the prioritization and coordination of these efforts within the framework of a common, nationwide vision.

The OIC will include a program management office responsible for coordinating the activities of the various portfolios. In addition, a cross-departmental coordinating council or interagency interoperability policy board, chaired by the Undersecretary for S&T, will be established to ensure that its efforts are coordinated intra- and inter-departmentally. This board will help reduce duplication in programs and activities.

With respect to specific tasks, the new OIC has already, at the direction of the Secretary of Homeland Security, undertaken a major initiative – RapidComm 9/30 – to achieve near term, emergency, incident-level interoperability in ten high threat urban areas by September 30, 2004. Working with multiple relevant Federal agencies, including the ODP, the Department of Justice, and the National Guard, we have begun working with all ten urban areas to identify what is in place, what is available, and what is still needed to provide interoperability to support a major incident.

Players: Owners, Partners, and Stakeholders

Those with a vested interest in the interoperability office include the people, agencies, and organizations that will directly benefit from enhanced interoperability of equipment and processes. Creating interoperability requires coordination and partnerships among office managers, partners, and stakeholders. Secretary Ridge has directed that S&T, as

the manager—or owner—of OIC, establish partnerships with all relevant offices and agencies in order to effectively coordinate similar activities. These partners will be instrumental in ensuring that our programs address all possible issues, ranging from grants for equipment procurement to regulatory policy creation. These partners and additional relevant stakeholders include representatives from the following communities:

- Emergency response providers represented by their national associations
- Department of Homeland Security and other government agencies
 - Operational programs and offices
 - Research & development offices
 - Test & evaluation programs
 - Technical assistance providers
 - Grant programs;
- Standards Development Organizations; and
- Industry

Principles for Achieving Interoperability

In order for the OIC to effectively coordinate and validate the Department’s interoperability programs, it will need to employ a common set of standards, policies, and procedures. This will require that the program employ a user driven approach and recognize the substantial investments that public safety and homeland security agencies have already made in existing equipment and procedures. Additionally, OIC must recognize the challenges associated with incorporating legacy equipment and practices in the face of constantly changing technology. Driving principles behind the management of this office include:

1. *Recognizing that it must be a user driven program* - Emergency response providers and homeland security practitioners – who own, operate and maintain more than 90% of the nation’s wireless public safety infrastructure – will be integrated into the program from its beginning, thereby allowing the program to create solutions that meet their needs. The public safety community will be involved primarily through associations. There are two reasons for this approach. First, the associations represent the leadership of their respective constituencies; and second, as the National Task Force on Interoperability (NTFI) has demonstrated, the associations are an excellent way to reach out to these communities.

2. *Extensive leveraging of what exists* - Cooperation and coordination with existing programs reduces unnecessary duplication of effort and increases efficient use of Federal resources dedicated to common causes. In addition, the investments that many public safety agencies have already made must be maximized.
3. *A standards-based approach* - Standards maximize competition across industry, encourage technology innovation, create an overall cost savings, and increase compatibility among public safety and homeland security agencies.
4. *Compliance with key policy documents and initiatives* – Compliance with the National Incident Management System, the National Response Plan, and relevant Homeland Security Presidential Directives will provide a consistent nationwide approach for agencies at all levels of government to work effectively and efficiently together to prepare for, prevent, respond to, and recover from major incidents.
5. *An effective outreach program* - Outreach efforts will emphasize the need for interoperability, and tools for its implementation, to practitioners and policy makers at all levels of government, and the public safety community.

The Communications Portfolio - SAFECOM

The Communications Portfolio, will continue to build on SAFECOM's achievements in bolstering public safety communications.

As a public safety practitioner driven program, and as part of the interoperability office, SAFECOM is working with existing Federal communications initiatives and key public safety stakeholders to address the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing communications systems and future networks. The customer base includes more than 50,000 State and local public safety agencies and organizations. Federal customers include more than 100 agencies engaged in public safety disciplines such as law enforcement, firefighting, public health, and disaster recovery. SAFECOM, and OIC are also working closely with the FCC to identify interoperability solutions for the first responder community. Recently the SAFECOM Program and the FCC agreed to set up a joint interoperability task force and have identified its first members in an effort to enhance achieving this objective. This task force will be formalized in the near future.

SAFECOM's objectives include: (1) developing standards in partnership with Federal, State, local and Tribal public safety organizations to define the requirements for first responder interoperability at all levels; (2) building from those standards, developing an architectural framework in coordination with the work under the National Response Plan to assist in the progression towards wireless interoperability; and (3) developing and implementing a process to coordinate the Federal Government's wireless interoperability investments and programs.

In addition, key challenges in achieving improved public safety communications and interoperability include both the lack of and fragmentation of spectrum. From the 1920's, when two-way radio communication began, spectrum was allocated as needed with little planning and no consideration of cross-jurisdictional interoperability. Originally, as the National Task Force on Interoperability (NTFI) report released in February 2003 has observed, almost all public safety communications were originally confined to the low end of the frequency range. As technology improved and increasing numbers of agencies began to set up radio communications systems, more radio spectrum was required and transmission at higher frequencies became both necessary and technologically possible. Hence, the FCC assigned frequencies in different bands, offering a temporary solution for congestion and crowding. The result is that public safety currently operates in ten separate bands, which has contributed to the fragmentation that characterizes public safety spectrum today and the consequent lack of public safety interoperability. On-going problems related to interference, overcrowding, and proprietary solutions still hamper the most effective use of the limited and fragmented public safety spectrum.

Spectrum issues are not simply technical problems requiring engineering solutions. Policies surrounding the use of spectrum—a limited resource sought by competing private and governmental interests—restrict public safety's ability to use it more efficiently. For example, in 1997, Congress allocated 24 MHz of spectrum in the 700 MHz band specifically to public safety. However, most of the 700 MHz spectrum allotted to public safety is currently unavailable for public safety because of television broadcasts on channels 63, 64, 68, and 69, especially in major metropolitan areas. Although this spectrum is scheduled to be available for public safety use on January 1, 2007, television stations are permitted to stay in the 700 MHz band until 85 percent of the households in their market areas have televisions capable of receiving digital television (DTV) signals. Currently only 14 percent of the current television sets in the U.S. are capable of receiving DTV signals. The result is that public safety is unable to make use of this much needed spectrum, on which lives may depend in daily public safety operations, and during times of disaster.

Spectrum policy is an essential issue in the public safety communications arena. Unfortunately, State and local public safety representatives are frequently not included in spectrum policy decisions, despite their majority ownership of the communications infrastructure and their importance as providers of public and homeland security. SAFECOM will hence play a key role in representing the views of State and local stakeholders on spectrum issues within the Federal Government. Last year, SAFECOM was appointed to an interagency Spectrum Task Force to contribute such views, and the ongoing working relationship that has developed between SAFECOM and the FCC will, we believe, pay huge dividends in the future. With the FCC's recent decision on the 800 MHz interference issue, we join with the public safety community in applauding the Federal Government's efforts to address public safety needs.

SAFECOM Achievements To Date

Over the last year, SAFECOM has made significant progress in both achieving its short-term goals and building the foundation for a comprehensive longer term program. It has established itself as the umbrella program within the Federal government for coordination with Federal, State, local and Tribal public safety agencies to improve public safety communication and interoperability.

- *Coordinated Funding Assistance* - In FY 2003, SAFECOM developed grant guidance in keeping with the needs of public safety for use by Federal programs funding public safety communications equipment to State and local agencies. Community Oriented Policing Services (COPS), Federal Emergency Management Agency (FEMA), and ODP incorporated this guidance into their public safety communications grants. This guidance marked the first coordinated approach to funding requirements. In further support of the coordinated grant process, SAFECOM organized and funded the peer review process for the joint grant solicitation from COPS and FEMA. SAFECOM also supported the Department of Commerce National Institute of Standards and Technology (NIST) Summit on Interoperability that was the first step towards identifying all the Federal and national programs involved in public safety communications so that a broader coordination effort can continue.
- *Statement of Requirements Development* - SAFECOM recently developed the Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability in coordination with the National Public Safety Telecommunications Council, NIST, and the Department of Justice's CommTech Program (formerly the AGILE Program). The SoR contains interoperability scenarios describing how SAFECOM envisions technology enhancing public safety. From these scenarios, operational requirements are defined and functional requirements of the technologies are extrapolated. The requirements identified in the SoR will drive the development and creation of interface standards that will satisfy public safety practitioner needs. The SoR will also offer industry a resource for understanding the users' needs in the development of new technologies and serve as a guide for SAFECOM to develop its research development, test, and evaluation program and constitutes the first national definition of what interoperability must accomplish. Using the requirements detailed in the SoR as the basis, SAFECOM is currently working with state and local public safety practitioners to develop an interoperability architectural framework. This framework provides a description of how the requirements detailed in the SoR support nationwide interoperability, allowing different state and local communications systems to interoperate in a system-of-systems network. A draft of the Architectural Framework will be completed by the end of 2004.

- *SAFECOM Strategic Plan Update* - SAFECOM conducted a strategic planning session at the Executive Committee (EC) and Advisory Group (AdG) meetings in June, 2004. The EC and AdG are comprised of senior level stakeholders from the Federal, State and local public safety communications communities. The strategic initiatives developed at the December Joint Planning Meeting were reviewed, and new objectives for the short and long term goals of the program were developed. SAFECOM is currently producing and will soon distribute a modified strategic plan based on stakeholder comments presented at these meetings.

SAFECOM On Track to Achieve Critical Milestones in 2004, including (but not limited to):

Detailed Interoperability Project Plan for the Commonwealth of Virginia

- SAFECOM will develop a detailed project plan using the result of the strategic planning session and the project team's technical expertise. This project plan will include tasks that need to be accomplished by the Commonwealth along with realistic timeframes for completion. Like the Virginia Strategic Planning Session, this plan will serve as a model for other states as they work towards achieving communications interoperability for public safety first responders.

Interoperability Grant Peer Review

- SAFECOM will facilitate interoperability grant peer review sessions enabling public safety communications subject matter experts to evaluate and comment upon grant applications for FY 2004 COPS and FEMA communications equipment grants. These reviewers will ensure that grants will be distributed only for projects that meet SAFECOM developed interoperability requirements.

RapidCom9/30

- SAFECOM is undertaking an initiative to ensure a minimum level of public safety interoperability is in place in ten key urban areas by September 30, 2004. The RapidCom9/30 project will provide incident commanders in charge of managing/directing various responding agencies the ability to adequately communicate with each other and the respective command center within one hour of an incident. Due to this effort's limited scalability, it is not meant to serve as a comprehensive public safety communications solution, but as an interim solution that provides a minimum-level interoperability capability during emergency responses.

Narrowbanding Report

- SAFECOM will release a report detailing the program's recommendations on spectrum policy in regard to narrowbanding in the 700 MHz band. As recent events in the 800 MHz band have shown, coordinated spectrum policy is important for public safety communications, and SAFECOM's input to any plan in the 700 MHz band will allow for more efficient spectrum use when allocated frequencies become available in the next decade.

National Guard Study

- SAFECOM will release a report outlining how National Guard Land Mobile Radio (LMR) resources can be incorporated into the plan to achieve nationwide interoperability. It will also identify how local public safety organizations can leverage National Guard assets. The National Guard already has a great deal of investment in LMR facilities, and this report will help local and state public safety organizations utilize resources that may already be present in their communities.

Communication Device Report

- SAFECOM will release a report detailing the findings of its testing and evaluation program. The first report will focus on the performance of public safety communications equipment with the P25 Phase I standard. This report is the first step in developing a comprehensive national architecture plan for communications interoperability.

Portal for Interoperability Information

- The Web Portal of Interoperability Information will be the "One-Stop-Shop" for information pertaining to public safety communications interoperability. As a portal, it will be an interactive community space, allowing registered users to research potential solutions as well as share their thoughts on existing technologies. Version 1.0 of this portal, which will be released in November 2004 is the first attempt to provide first responders with a central repository of critical information pertaining to communications interoperability.

National Interoperability Baseline Methodology

- SAFECOM will release a methodology detailing how a baseline of the level of interoperability nationwide can be established. The baseline is required in order to understand the current level of interoperability at the local and State levels and will be used to measure the success of the SAFECOM Program in achieving national communications interoperability for first responders in the coming years.

Conclusion

Our Nation is heavily invested in an existing infrastructure that is largely incompatible. As I stated earlier, current efforts within the Federal Government to address the interoperability problem are being coordinated to incorporate the needs of Federal, State and local practitioners. We must continue to pursue the current comprehensive strategy that takes into account technical and cultural issues associated with improving communications and interoperability, and recognizes the challenges associated with incorporating legacy equipment and practices given the constantly changing nature of technology.

The many obstacles facing public safety interoperability make for complex problems with no one-size-fits-all solution. Flexible and dynamic solutions are necessary to combat the unique challenges presented by the first responder world. The new OIC and its partners will continue to work towards a world where lives and property are never lost unnecessarily because public safety agencies are unable to communicate or lack compatible equipment and training resources.