AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

PROJECT SAFECOM: MORE TIME, MORE MONEY, MORE COMMUNICATION? WHAT PROGRESS HAVE WE MADE IN ACHIEVING INTEROPERABLE COMMUNICATION BETWEEN LOCAL, STATE AND FEDERAL FIRST RESPONDERS?

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SEPTEMBER 8, 2004

Serial No. 108–264

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

98–292 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
BETTY MCCOLLUM, Minnesota

BERNARD SANDERS, Vermont (Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
BETTY MCCOLLUM, Minnesota

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
SHANNON WEINBERG, *Professional Staff Member/Deputy Counsel*
JULIANA FRENCH, *Clerk*
ADAM BORDES, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on September 8, 2004	1
Statement of:	
Beres, Timothy L., Associate Director, Office for Domestic Preparedness, Department of Homeland Security	49
Boyd, David G., Ph.D., Director, SAFECOM Program Office, Science and Technology Directorate, Department of Homeland Security	37
Jenkins, William O., Jr., Director, Homeland Security and Justice Issues, U.S. Government Accountability Office	11
Lischke, Maureen, Senior Executive Service, Chief Information Officer, National Guard Bureau	102
Muleta, John, esq., Chief, Wireless Telecommunications Bureau, Federal Communications Commission	71
Neuhard, Michael P., fire chief, Fairfax County Fire and Rescue Department	121
Stile, Vincent, past president, Association of Public Safety Communications Officials International, Inc.	110
Worden, Thomas B., chief, Telecommunications Branch, State of California, Governor's Office of Emergency Services	128
Letters, statements, etc., submitted for the record by:	
Beres, Timothy L., Associate Director, Office for Domestic Preparedness, Department of Homeland Security, prepared statement of	51
Boyd, David G., Ph.D., Director, SAFECOM Program Office, Science and Technology Directorate, Department of Homeland Security, prepared statement of	40
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	8
Jenkins, William O., Jr., Director, Homeland Security and Justice Issues, U.S. Government Accountability Office, prepared statement of	14
Lischke, Maureen, Senior Executive Service, Chief Information Officer, National Guard Bureau, prepared statement of	104
Muleta, John, esq., Chief, Wireless Telecommunications Bureau, Federal Communications Commission, prepared statement of	74
Neuhard, Michael P., fire chief, Fairfax County Fire and Rescue Department, prepared statement of	124
Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of	4
Stile, Vincent, past president, Association of Public Safety Communications Officials International, Inc., prepared statement of	112
Worden, Thomas B., chief, Telecommunications Branch, State of California, Governor's Office of Emergency Services, prepared statement of	131

PROJECT SAFECOM: MORE TIME, MORE MONEY, MORE COMMUNICATION? WHAT PROGRESS HAVE WE MADE IN ACHIEVING INTEROPERABLE COMMUNICATION BETWEEN LOCAL, STATE AND FEDERAL FIRST RESPONDERS?

WEDNESDAY, SEPTEMBER 8, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 2 p.m., in room 2154, Rayburn House Office Building, Hon. Adam H. Putnam (chairman of the committee) presiding.

Present: Representatives Putnam, Miller, Clay, and McCollum.

Staff present: Bob Dix, staff director; John Hambel, senior counsel; Shannon Weinberg, professional staff member/deputy counsel; Juliana French, clerk; Grace Washbourne, professional staff member, full committee; Adam Bordes, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. PUTNAM. Good afternoon, and welcome. This hearing of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good afternoon and welcome to the subcommittee's hearing on "Project SAFECOM: More Time, More Money, More Communication? What Progress Have We Made in Achieving Interoperable Communication Between Local, State and Federal First Responders?"

The purpose of this hearing is to discuss the status and progress of achieving communications interoperability among the various first responders and to continue the subcommittee's oversight of related Federal, State and local government programs. Specifically, this hearing will review the progress of Project SAFECOM, one of the President's 25 Quicksilver e-Government initiatives, in developing policies that encourage State and local agencies to work together to promote first responders communications interoperability.

In its short history, Project SAFECOM has been relocated to three different agencies, with four different management teams. Now at the Department of Homeland Security, the initiative appears to be progressively moving forward. In April of this year, Project SAFECOM adopted the statement of requirements for wire-

less public safety communications and interoperability. What remains unclear, however, is the status of implementation of these standards.

Interoperable communications is the ability of first responders to share time sensitive information across disciplines and jurisdictions via communications systems in real time. On September 11, 2001, we witnessed a failure in communication not only among differing first responder agencies, but within the responding agencies themselves. The tragic loss of so many lives was among the most shocking events in our modern history. The tragedy of this event is compounded by the knowledge that the loss of many lives, particularly those of numerous first responders, could have been prevented had there been fully interoperable communications.

Interoperability is not only important in managing a terror-related incident, but also critical in answering the call of other emergencies. Federal, State and local governments work together to answer many other types of emergencies. Here in our Nation's capital, we have the U.S. Park Police, the U.S. Capitol Police and the Metropolitan Police Department working together on a regular basis for crowd control at celebrations and demonstrations. The 2003 wildfires in San Diego, California drew response teams from a number of Federal, State and local agencies, as well as other States. And more recently, in my home area in Florida, twice in the last 25 days, numerous Federal, State and local agencies have worked together to evacuate 47 out of our 67 counties, nearly 3 million people in the State's largest ever evacuation for Hurricane Frances, only 3 weeks after evacuating nearly 1 million people for Hurricane Charley.

The vast majority of infrastructure for these interoperable communications resides in the management of the State and locals. Consequently, the Federal Government's role through Project SAFECOM is that of facilitating the development of the communication across the Nation. Frequently, we have support and response from other States coming in to support local responders in a major emergency.

Through standards development and implementation, the goal of Project SAFECOM is to avoid situations in which the only way to communicate emergency response efforts is by switching a handheld radio between responding agencies. By encouraging the adoption of standards, the hope is that cash-strapped local governments will not spend tens of millions of dollars on communications systems that prove to not be interoperable with surrounding counties.

For instance, in the San Diego, California example, in October they were hit by the most devastating wildfire disaster in their history. Three major fires raged across the county, killing 16, leaving more than 390,000 acres burned and 2,700 residential or commercial buildings destroyed. The comprehensive study of that firestorm declared that better communication was necessary. Not all firefighters had uniform ability to communicate, first because while county fire agencies used spectrum in the 800 megahertz frequency, State and Federal agencies use a VHF system.

Further, some officials report that in that incident, their $90 million regional communication system proved to be ineffective, or at the least it performed sub-par in this and other major catastrophes.

The system was first used in 1998 and was meant to enable 80 county, local and State government agencies, such as sheriffs, deputies and firefighters to communicate during emergencies.

But during the firestorm of 2003, the system was plagued by busy signals, 38,000 in the south county and 68,000 in the east county. While fire administrators and many county officials say the system is better than what they had before, that's not good enough given the state of technology and the state of perpetual danger today. We can and must do better.

With the interoperable communication and homeland security grants available to State and local governments, now centralized under DHS within the Office of Domestic Preparedness, it appears that the Department of Homeland Security has the carrot to persuade State and local governments to adopt the standards developed by Project SAFECOM. This appearance may be an illusion, however, because the grant money is awarded in the form of a block grant with few opportunities to follow up to ensure that the standards tied to those grants are actually adopted or implemented.

Last November, this subcommittee held a joint hearing with the Subcommittee on National Security and Emerging Threats to discuss the challenges of achieving first responder interoperable communications. Today's hearing is an opportunity to examine those continued efforts to measure the progress and to determine the next steps in not only Project SAFECOM but other Federal, State and local efforts.

As several offices still play a role in achieving communications interoperability, this hearing also provides an opportunity to examine cross-agency coordination in this effort. We have two very distinguished panels of witnesses today, the first comprised of representatives from the Federal offices working on communications interoperability, and I am eager to hear about the current state of their efforts in achieving an interoperable communications network of first responders.

Our second panel is comprised of a number of Federal, State and local officials who either work on the government side of communications interoperability or who have first-hand disaster management experience, involving multiple response teams. One of our panelists, Larry Alexander from Polk County, FL, was prepared to give us first-hand disaster management expertise but he is still managing a disaster with multiple Federal, State and local agencies as we speak, as part of the recovery operations center in the aftermath of Hurricane Frances and in preparation potentially for Hurricane Ivan.

We look forward to the expert testimony of those who are able to join us today. I'm pleased to be joined by our distinguished ranking member, the gentleman from Missouri, Mr. Clay and our distinguished Vice Chair from Michigan, Ms. Miller. At this time, I would yield to Mr. Clay for any opening remarks he may have. You're recognized.

[The prepared statement of Hon. Adam H. Putnam follows:]

TOM DAVIS, VIRGINIA
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
Congressman Adam Putnam, Chairman

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic:

"Project SAFECOM: More time. More money. More communication? What progress have we made in achieving interoperable communication between local, state, and federal first responders?"

Wednesday, September 8, 2004
2:00 p.m.
Room 2154, Rayburn House Office Building

OPENING STATEMENT

Good afternoon and welcome to the Subcommittee's hearing on *"Project SAFECOM: More time. More money. More communication? What progress have we made in achieving interoperable communication between local, state, and federal first responders?"*

The purpose of this hearing is to discuss the status and progress of achieving communications interoperability among federal, state, and local first responders and to continue the Subcommittee's oversight of related federal, state, and local government

programs. Specifically, this hearing will review the progress of Project SAFECOM, one of the President's 25 Quicksilver e-Government initiatives, in developing policies and regulations that encourage state and local agencies to work together to promote and establish first responder communications interoperability. In its short history, Project SAFECOM has been relocated to three different agencies with four different management teams. Now at the Department of Homeland Security (DHS), the initiative appears to be progressively moving forward. In April 2004, Project SAFECOM adopted the "Statement of Requirements for Wireless Public Safety Communications and Interoperability." What remains unclear, however, is the status of implementation of these standards. Where are we now?

Interoperable communications is the ability of first responders to share time-sensitive information across disciplines and jurisdictions via communication systems in real time. On September 11, 2001, we witnessed a failure in communication not only among differing first responder agencies, but within the responding agencies themselves. The tragic loss of many lives was the most shocking event in our modern history. The tragedy of this event is compounded by the knowledge that the loss of many lives, particularly those of numerous first responders, could have potentially been prevented had there been fully interoperable communications.

Interoperability is not only important in managing a terror-related incident; it is also critical in answering the call of other emergencies. Federal, state, and local governments work together to answer many other types of emergencies. Here in our Nation's capital, we have the US Park Police, the US Capitol Police, and the Metropolitan Police Department working together frequently for crowd control at celebrations or for demonstrations. The 2003 wildfires of San Diego drew response teams from numerous federal, state, and local agencies, as well as from numerous other states. Most recently, in Florida, numerous federal, state, and local agencies worked together to evacuate 47 out of 67 counties, close to *2.8 million* people, in the state's largest ever evacuation for Hurricane Frances, only three weeks after approximately 1 million people were evacuated for Hurricane Charley.

The vast majority of infrastructure for these interoperable communications resides under the management of state and local responders. Consequently, the federal government's role through Project SAFECOM is one of facilitating the development of interoperable communication across the nation. Through standards development and implementation, the goal of Project SAFECOM is to avoid situations in which the only way to communicate and coordinate emergency response efforts is by switching a hand-held radio between responding agencies. By encouraging the adoption and implementation of standards, the hope is that cash-strapped local governments will not spend tens of millions of dollars on communications systems that prove to not be interoperable with surrounding counties. For instance, in October 2003, San Diego County was hit by the most devastating wildfire disaster in California history. Three major fires raged across the county, killing 16 people, leaving more than 390,000 scorched acres, and nearly 2700 residential or commercial buildings destroyed with many more damaged. In January 2004, a comprehensive study of Firestorm 2003 declared that better communication was necessary. Not all firefighters had uniform ability to communicate, first because while county fire agencies use spectrum in the 800 MHz radio frequency, state and federal agencies use a VHF system. Further, some officials report that San Diego County's $90 million regional communications system proved to be ineffective, or at the least, had performed sub par, in this and other major catastrophes. The system was first used in

1998 and was meant to enable 80 local, county, and state government agencies such as sheriff's deputies and firefighters to communicate during major emergencies. During Firestorm 2003, the system was plagued by busy signals – 38,000 in the South County and 68,000 in the East County. While fire administrators and many county officials say the system is better than what they had before, that is simply not good enough given the state of technology and the state of perpetual danger today – we *can* and *must* do better.

With the interoperable communications and homeland security grants available to state and local governments now also centralized under DHS within the Office of Domestic Preparedness (ODP), it appears that DHS has the "carrot" to persuade state and local governments to adopt the standards developed by Project SAFECOM. However, this appearance may prove to be an illusion because the grant money is awarded in the form of a block grant, with few opportunities to follow up to ensure that the standards tied to those grants are actually adopted and implemented.

Last November this Subcommittee held a joint hearing with the Subcommittee on National Security, Emerging Threats and International Relations to discuss the challenges of achieving first responder interoperable communications. Today's hearing is an opportunity to examine the continuing efforts, to measure the progress, and to determine the next steps in not only Project SAFECOM, but also in other federal, state, and local efforts. As several federal offices still play a role in achieving communications interoperability, this hearing also provides an opportunity to examine cross-agency and intergovernmental coordination in this effort.

We have two distinguished panels of witnesses today, the first comprised of representatives from the several federal offices working for communications interoperability. I am eager to hear about the current state of their efforts in achieving a fully interoperable communications network of first responders. Our second panel is comprised of a number of federal, state, and local officials who either work on the governance side of communications interoperability or who have first-hand disaster management experience involving multiple response teams. I eagerly look forward to the expert testimony these distinguished panels of leaders will provide today.

#####

Mr. CLAY. Thank you, Mr. Chairman for calling this hearing on what is a critical issue to our national welfare. Let me also say that we're glad to see you back here in one piece, and to know that your family and constituents are safe from the two hurricanes that occurred in Florida and from what we hear, an expected third one, and let you know that we are glad you are here.

This is not the first time our subcommittee has addressed the issues of communication and interoperability and substandard management within the organizations that our citizens depend on in times of crisis. It is my hope that our efforts today will aid all stakeholders in establishing long-term policies and mechanisms for improved communications when we need them. To begin, I am dismayed by the recent findings of GAO with regard to the lack of cooperation among Federal agencies having responsibility for both financing and operations of Project SAFECOM. As a starting point for its troubles, the program has undergone various changes in management and oversight since its creation 3 years ago, having been assigned and reassigned among three different agencies and four separate management teams. Although management of the multi-agency project now permanently resides in the Department of Homeland Security, past efforts have been ineffective for managing a program that is designed to coordinate the efforts of our Nation's first responders.

Further complicating matters is DHS' failure to secure operational and financial agreements among several of its partnering agencies on SAFECOM initiatives. While DHS has placed significant effort into its role as managing partner of SAFECOM, it cannot hold the system together without the cooperation and financial support of other stakeholders throughout the Federal, State and local bureaucracy.

Until such financial and operational mechanisms are agreed to among SAFECOM stakeholders, the project will continue to be underfunded on an annual basis, fail in its attempt to define and implement national standards for wireless interoperability and lose the confidence of all other stakeholders in its mission as a central coordinator for responding to local and national crises.

Again, thank you, Mr. Chairman, for calling this hearing and I look forward to the testimony from the witnesses.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

**STATEMENT OF THE HONORABLE WM. LACY CLAY
AT THE HEARING ON
PUBLIC SAFETY INTEROPERABILITY**

September 8, 2004

Thank you, Mr. Chairman, for calling this hearing on what is a critical issue to our national welfare. This is not the first time our subcommittee has addressed the issues of communications interoperability and substandard management within the organizations that our citizens depend on in times of crisis. It is my hope that our efforts today will aide all stakeholders in establishing long-term policies and mechanisms for improved communications when we need them.

To begin, I am dismayed by the recent findings of GAO with regard to the lack of cooperation among federal agencies having responsibility for both the financing and operations of Project SAFECOM. As a starting point for its troubles, the program has undergone various changes in management and oversight since its creation three years ago--having been assigned and reassigned among three different agencies and four separate management teams. Although management of the multi-agency project now permanently resides in the Department of Homeland Security, past efforts have been ineffective for managing a program that is designed to coordinate the efforts of our nation's first responders.

Further complicating matters is DHS's failure to secure operational and financial agreements among several of its partnering agencies on SAFECOM initiatives. While DHS has

placed significant effort into its role as managing partner of SAFECOM, it cannot hold the system together without the cooperation and financial support of other stakeholders throughout the federal, state, and local bureaucracy.

Until such financial and operational mechanisms are agreed to among SAFECOM stakeholders, the project will continue to be under funded on an annual basis, fail in its attempts to define and implement national standards for wireless interoperability, and lose the confidence of all other stakeholders in its mission as a central coordinator for responding to local and national crises.

Again, thank you Mr. Chairman for calling this hearing, and I look forward to the testimony from the witnesses.

Mr. PUTNAM. Thank you, Mr. Clay.

The gentlelady from Michigan, Ms. Miller.

Ms. MILLER. Thank you, Mr. Chairman. I certainly want to tell you how much I appreciate you holding this hearing and how very much we all appreciate you actually attending, considering what you have just been through. As Mr. Clay mentioned as well, I think the audience needs to recognize our chairman just literally got off the airplane. He's too modest to tell you that, but about 20 minutes ago, because that hurricane hit his county very, very severely, Polk County and in that immediate area. And I know that all the members of both chambers were very happy to authorize additional expenditures for the State of Florida. They've been so hard hit with these two last hurricanes and another one coming. So we appreciate your attendance here today and your commitment and your dedication to that. Certainly our thoughts and prayers are with everybody in Florida and hopefully Ivan doesn't get there. But in the interim, having this hearing today I think is very appropriate, very timely as we discuss this particular issue.

Our Nation's war on terror has certainly placed our Nation at a pivotal moment in history, quite frankly. Brave men and women are fighting for our freedoms across our entire globe. But our enemy seeks to take the fight to our homeland as well. And first responders, of course, as often, and we certainly witnessed that on September 11, are the very first line of defense.

Historically, we've considered, of course, police and firefighters as our Nation's first responders. But with today's threats, individuals such as health care officials and utility workers and others as well are also now going to be called first responders. I think they will certainly be called to duty in the event of an emergency. And it's vital to support these individuals in order to recover quickly from an urgent situation and to minimize its impact.

Project SAFECOM is one aspect where the Federal Government can offer a considerable amount of support to State and local governments as they prepare their first response teams. Interoperable communication between Government agencies and organizations is vital to emergency response, it has to be done very quickly, especially with the availability of new technologies. We need to be able to utilize those technologies.

State and local government support the necessary infrastructure, but the Federal Government, our role certainly is to offer them all guidance and set some standards. Upon reviewing the written testimony of today's witnesses, I am cautiously optimistic that Project SAFECOM is on the right track, and I certainly look forward to the testimony that we'll have from our panels today.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you very much, Ms. Miller.

At this time we will move directly into testimony. I would ask our first panel to please rise and raise your right hands, and anyone accompanying you who will be providing information for your answers to be sworn in as well. Please raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. I note for the record that all the witnesses responded in the affirmative. And we will move directly to testimony, beginning with Mr. William Jenkins. Mr. Jenkins currently serves

as the Director of Homeland Security and Justice Issues within the U.S. Government Accountability Office. In this position, he is responsible for issues regarding emergency preparedness and response, elections, Federal Judiciary sentencing and corrections and bankruptcy. Prior to joining GAO as a faculty fellow in 1979, Mr. Jenkins was a professor of political science. He has also served as an adjunct professor to the American University. His principal areas of concentration include budget policy, defense, administration of justice and homeland security. He is a graduate of Rice University and received his M.A. of political science and Ph.D. in public law from the University of Wisconsin at Madison.

We have a room issue, we will be doing everything we can to move the hearing along, and we would ask all of our witnesses to please abide by the 5-minute rule. Mr. Jenkins, you are recognized for 5 minutes.

STATEMENT OF WILLIAM O. JENKINS, JR., DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. JENKINS. Thank you, Mr. Chairman and members of the subcommittee.

I appreciate the opportunity to be here today to discuss our work on wireless interoperable communications for first responders. First, it's important to note that interoperable communications is not an end in itself and is not primarily a technology issue. Rather, it is a necessary means of achieving an important goal, the ability to respond effectively to and mitigate the effects of incidents that require the coordinated actions of first responders. Interoperable communications is but one important component of an effective incident command and operation structure.

Achieving effective interoperable communications for first responders requires the successful integration of people, processes and technology. The technology needed flows from a comprehensive assessment of needs and the incident management structure in which the technology will be used.

In our July 2004 report and November 2003 testimony before this subcommittee, we outlined three challenges in achieving interoperable communications that remain the principal challenges today. They are, one, clearly defining and identifying the problem; two, establishing performance goals, requirements and standards; and three defining governmental roles and addressing the problem. These are primarily people and process issues.

The single biggest obstacle to achieving effective interoperable communications has been and remains the lack of effective, collaborative, interdisciplinary and intergovernmental planning. The cultural and turf barriers for achieving this are deeply rooted and longstanding.

Second, Federal, State and local governments all have important roles to play in developing standards that can be used to assess interoperability requirements, identify gaps in the current ability to meet those requirements and develop and implement comprehensive plans for closing those gaps. The Federal Government could provide the leadership, focus and long term commitment needed.

For example, it could take leadership in developing a set of baseline requirements, a national data base of interoperable frequencies, a national standard nomenclature for those frequencies, and a governance and funding structure that supports State efforts to develop and implement statewide interoperable communication plans.

Moreover, only the Federal Government can allocate public safety spectrum. With support from the Federal Government and broad participation and input from local and tribal governments and first responders, States can serve as the focal points for statewide interoperability planning and implementation. The FCC has recognized the States' importance by providing the States authority to administer the interoperability channels within the 700 megahertz spectrum. Some States are working to develop statewide plans, but there is no established structure or funding to support such efforts. Nor is there any guidance for States on what should be included in such plans. Such plans would need to encompass cross-State interoperability issues in such areas as New York, Philadelphia and Cincinnati, where metropolitan areas cross State boundaries.

SAFECOM was established as the umbrella program for coordinating all Federal initiatives and projects on public safety interoperable communications. According to SAFECOM, there are more than 100 Federal agencies and programs involved in public safety issues. SAFECOM's ability to provide the needed Federal leadership and coordination has been hampered by its dependence on other Federal agencies for funding and cooperation. DHS has recently created the Office of Interoperability and Compatibility to be fully established by November 2004. However, that office's structure, funding and authority are still being developed.

The status of current interoperable communications capabilities nationwide, including the scope and severity of any shortcomings, has not yet been determined. To assess these capabilities, a set of requirements is needed that can be used to assess what is compared to what should be. In April 2004, SAFECOM issued a document designed to serve as a set of baseline requirements, expects to complete its baseline assessment of current interoperable capabilities by July 2005, but is still refining its methodology for developing that baseline.

Third and finally, the fragmented Federal branch structure for first responders limits the Federal Government's ability to provide consistent, effective guidance and support for State and local planning and implementation efforts. SAFECOM has developed recommended grant guidance for all Federal grants whose moneys could be used to improve interoperability But cannot require consistent guidance be included in all Federal first responder grants.

Moreover, some grants do not support long term planning efforts. For example, they do not require interoperable communications plans prior to receiving funds or have a 1 or 2 year performance period that may encourage a focus on equipment purchases rather than comprehensive planning to guide those purchases.

In addition, Federal and State Governments lack a coordinated grant review process to ensure that funds allocated to local governments are used for communications projects that complement each other and add to overall statewide and national interoperable ca-

pacity. One result is that grants could be approved for bordering jurisdictions that propose conflicting interoperable solutions.

We recognize that SAFECOM has made progress in bringing leadership and focus to the Federal Government's interoperability efforts and many State and local officials are working diligently to assess and improve interoperable communications. Our July 2004 report includes recommendations to the Secretary of DHS and the Director of OMB for enhancing Federal coordination and providing assistance and encouragement to States to establish statewide interoperability planning bodies that draw on the experience and perspectives of local first responders.

That concludes my statement, Mr. Chairman, and I would be happy to answer any questions you or other members of the committee may have.

[The prepared statement of Mr. Jenkins follows:]

United States Government Accountability Office

GAO

Testimony Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EST
Wednesday, September 8, 2004

HOMELAND SECURITY

Federal Leadership Needed to Facilitate Interoperable Communications Between First Responders

Statement of William O. Jenkins, Jr.
Director, Homeland Security and Justice Issues

GAO-04-1057T

September 2004

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-04-1057T, a testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House of Representatives

HOMELAND SECURITY

Federal Leadership Needed to Facilitate Interoperable Communications Between First Responsders

Why GAO Did This Study

Lives of first responders and those whom they are trying to assist can be lost when first responders cannot communicate effectively as needed. This testimony addresses issues of determining the status of interoperable wireless communications across the nation, the potential roles that federal, state, and local governments can play in improving these communications, and the need to structure grant programs so that they better support public sector efforts to improve these communications.

What GAO Recommends

In a recent report on interoperable communications, we recommended that the Secretary of DHS (1) continue to develop a nationwide database and common terminology for public safety interoperability communications channels; (2) help states assess interoperability in specific locations against defined requirements; (3) through federal grant awards, encourage state action to establish and support a statewide body to develop and implement detailed improvement plans; and (4) require that grant applications be in compliance with statewide interoperability plans, once they are developed. GAO also recommends that the Director of OMB work with DHS to review SAFECOM's functions and establish a long-term program with appropriate authority and funding to coordinate interoperability efforts across the federal government.

www.gao.gov/cgi-bin/getrpt?GAO-04-1057T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact William O. Jenkins, Jr. at (202) 512-8777 or jenkinsjrw@gao.gov.

What GAO Found

The current wireless interoperable communications capabilities of first responders nationwide have not been determined. To assess these capabilities, a set of requirements is needed that can be used to assess "what is" compared to "what should be." The Office of Management Budget (OMB) has established the Wireless Public Safety Interoperable Communications Program, SAFECOM, within the Department of Homeland Security (DHS) as the focal point for coordinating federal efforts to improve interoperable communication. In April 2004, SAFECOM issued a document designed to serve as a set of baseline requirements and is working to develop a baseline of current capabilities by July 2005. This is a difficult task, and the details of SAFECOM's baseline study have yet to be finalized.

The federal government can take a leadership role and provide support for developing (1) a national database of interoperable communication frequencies, (2) a common nomenclature for those frequencies, (3) a national architecture that identifies communications requirements and technical standards, and (4) statewide interoperable communications plans. SAFECOM has limited authority and ability to oversee and coordinate federal and state efforts as it is dependent upon other agencies for funding and their willingness to cooperate. DHS, where SAFECOM now resides, has recently announced it is establishing an Office for Interoperability and Compatibility to coordinate the federal response to the problems of interoperability. The exact structure and funding for this office, which will include SAFECOM, are still being developed.

State and local governments can play a large role in developing and implementing plans to improve public safety agencies' interoperable communications. State and local governments own most of the physical infrastructure of public safety communications systems, and states play a central role in managing emergency communications. States, with broad input from local governments, are a logical choice to serve as a foundation for interoperability planning because incidents of any level of severity originate at the local level with states as the primary source of support. However, states are not required to develop interoperability plans, and there is no clear guidance on what should be included in such plans.

The federal funding assistance programs to state and local governments do not fully support regional planning for communications interoperability. Federal grants that support interoperability have different requirements to tie funding to interoperable communications plans. In addition, uncoordinated federal and state level reviews limit the government's ability to ensure that federal funds are used to effectively support improved regional and statewide communications systems.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to discuss the critical issue of wireless interoperable communications for first responders.[1] In a recent report, we addressed the importance of determining the status of interoperable wireless communications across the nation and defining the potential roles that federal, state, and local governments can play in improving these communications.[2] The inability of first responders—police officers, fire fighters, emergency medical service personnel, public health officials, and others—to communicate effectively over wireless systems with one another as needed during an emergency is a long-standing and widely recognized problem in many areas across the country. Lives of first responders and those whom they are trying to assist can be lost when first responders cannot communicate effectively as needed.

Public safety officials generally recognize that effective "interoperable" communications is the ability to talk with whom they want, when they want, when authorized, but not the ability to talk with everyone all of the time. The effective interoperability of wireless systems permits a rapid and coordinated response to an emergency incident, whether that incident is a "routine" spill from an overturned tanker truck or railcar, a natural disaster, or a terrorist attack. In this statement, we (1) discuss the current status of interoperable wireless communication between first responders across the nation, (2) identify areas in which the federal government can take a leadership role, (3) highlight the critical role that state and local governments can play in the emergency communications planning process, and (4) discuss the need to structure grant programs so that they better support long-term, ongoing, and sustainable public sector efforts to improve security.

[1]Our work addressed issues of public safety wireless communications interoperability—i.e., communications that use radio frequency waves instead of telephone wires for transmitting voice and data. We did not address interoperability problems that may be found in other homeland security functions, such as fire equipment, chem-bio equipment, and information technology.

[2]U.S. Government Accountability Office, *Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-740 (Washington, D.C.: July 2004).

In doing our work, we met with federal, state, and local officials,[3] obtained and reviewed appropriate documentation, attended several meetings of public safety communications officials, and met with staff of the National Governors Association. We conducted our work from July 2003 through August 2004 in accordance with generally accepted government auditing standards.

Summary

- The current wireless interoperable communications capabilities of first responders nationwide has not been determined. To assess these capabilities, a set of requirements is needed that can be used to assess "what is" compared to "what should be." The Office of Management and Budget (OMB) has designated the Wireless Public Safety Interoperable Communications Program (SAFECOM), within the Department of Homeland Security (DHS), as the focal point for coordinating federal efforts to improve interoperable communications. In April 2004, SAFECOM issued a document designed to serve as a set of baseline requirements and is working to develop a baseline of current capabilities by July 2005. This is a difficult task, and the details of SAFECOM's baseline study are still being worked out.

- The federal government can provide the leadership, long-term commitment, and focus to help state and local governments meet interoperability goals. For example, the federal government can provide the leadership and support for developing (1) a national database of interoperable communications frequencies, (2) a common nomenclature for those frequencies, (3) a national architecture that identifies communications requirements and technical standards, and (4) statewide interoperable communications plans.

- DHS has recently created the Office of Interoperability and Compatibility to coordinate the federal response to the problems of interoperability in several functions, including wireless communications. DHS expects the office to be fully established by November 2004. As of August 2004, the exact structure and funding for the office, including SAFECOM's role within the office, were still being developed.

- With input from local governments and first responders, states can serve as focal points for statewide planning to improve interoperable

[3]To examine potential roles that state and local governments can play in improving interoperability of first responder wireless communications, we interviewed state and local officials in California, Florida, Georgia, and Washington.

communications. States can play a key role in improving interoperable communications by establishing a management structure that includes local participation and input to analyze and identify interoperability gaps between "what is" and "what should be," developing comprehensive local, state, and regional plans to address such gaps, and funding implementation of these plans.

- The fragmented federal grant structure for first responders does not support statewide interoperability planning. SAFECOM has developed grant guidance for interoperability, but cannot require that consistent guidance be incorporated in all federal first responder grants. The structure of some federal grants does not support long-term planning efforts because, for example, they did not require a communications plan prior to receiving grant funds and required a 1- or 2-year performance period. The federal and state governments lack a coordinated grant review process to ensure that funds allocated to local governments are used for communication projects that complement each other and add to overall statewide and national interoperability capacity.

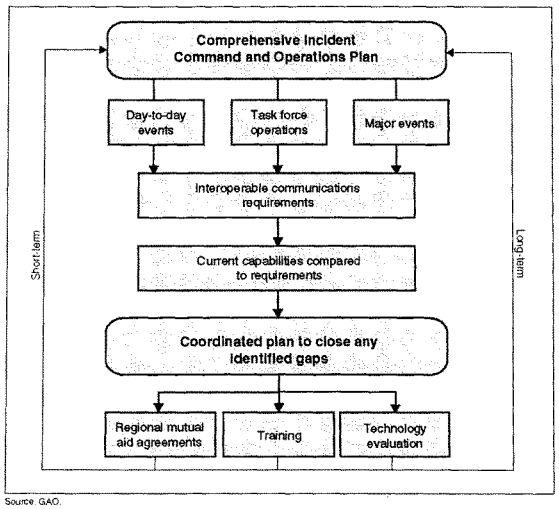
Background

Interoperable communications is not an end in itself. Rather, it is a necessary means for achieving an important goal—the ability to respond effectively to and mitigate incidents that require the coordinated actions of first responders, such as multi-vehicle accidents, natural disasters, or terrorist attacks. Interoperable communications are but one component, although a key one, of an effective incident command planning and operations structure. As shown in figure 1, determining the most appropriate means of achieving interoperable communications must flow from a comprehensive incident command and operations plan that includes developing an operational definition of who is in charge for different types of events and what types of information would need to be communicated (voice, data, or both) to whom under what circumstances. Other steps include:

- defining the range of interoperable communications capabilities needed for specific types of events;
- assessing the current capabilities to meet these communications needs;
- identifying the gap between current capabilities and defined requirements;
- assessing alternative means of achieving defined interoperable communications requirements; and
- developing and implementing a comprehensive plan—including, for example, mutual aid agreements, technology and equipment specifications, and training—for closing the gap between current capabilities and identified requirements.

Interoperable communications requirements are not static, but change over time with changing circumstances (e.g., new threats) and technology (e.g., new equipment) and additional available broadcast spectrum. Consequently, both a short- and long-term "feedback loop" that incorporates regular assessments of current capabilities and needed changes is important.

Figure 1: A Planning Process for Interoperable Communications



Source: GAO.

In addition, the first responder community is extensive and extremely diverse in size and the types of equipment in their communications systems. According to SAFECOM officials, there are over 2.5 million public safety first responders within more than 50,000 public safety organizations in the United States. Local and state agencies own over 90

percent of the existing public safety communications infrastructure. This intricate public safety communications infrastructure incorporates a wide variety of technologies, equipment types, and spectrum bands.[4] In addition to the difficulty that this complex environment poses for federal, state, and local coordination, 85 percent of fire personnel, and nearly as many emergency management technicians, are volunteers with elected leadership. Many of these agencies are small and do not have technical expertise; only the largest of the agencies have engineers and technicians.

In the past, a stovepiped, single jurisdiction, or agency-specific communication systems development approach prevailed—resulting in none or less than desired interoperable communications systems. Public safety agencies have historically planned and acquired communications systems for their own jurisdictions without concern for interoperability. This meant that each state and local agency developed communications systems to meet their own requirements, without regard to interoperability requirements to talk to adjacent jurisdictions.

For over 15 years, the federal government has been concerned with public safety spectrum issues, including communications interoperability issues.[5] A variety of federal departments and agencies have been involved in efforts to define the problem and to identify potential solutions, such as DHS, the Department of Justice (DOJ), the Federal Communications Commission (FCC), and the National Telecommunications and Information Administration (NTIA) within the Department of Commerce (DOC), among others. Today, a combination of federal agencies, programs, and associations are involved in coordinating emergency communications.

DHS has several agencies and programs involved with addressing first responder interoperable communication barriers, including the SAFECOM program, the Federal Emergency Management Agency (FEMA), and the

[4]Spectrum bands are the useable radio frequencies in the electromagnetic distribution. Specific frequencies have been allocated to the public safety community.

[5]The radiofrequency spectrum is the medium that enables wireless communications of all kinds. Although the radio spectrum spans the range from 3 kilohertz to 300 gigahertz, 90 percent of its use is concentrated in the 1 percent of frequencies that lie below 3.1 gigahertz, because these frequencies have properties that make this portion of the spectrum well suited for many important wireless technologies. Radio waves are a form of electromagnetic radiation that propagate in space as the result of particle oscillations. The number of oscillations per second is called "frequency," which is measured in units of hertz. The term "kilohertz" refers to thousands of hertz and "gigahertz" to billions of hertz.

Office for Domestic Preparedness (ODP). As one of its 24 E-Gov initiatives, OMB in 2001 created SAFECOM to unify the federal government's efforts to help coordinate the work at the federal, state, local, and tribal levels to establish reliable public safety communications and achieve national wireless communications interoperability. The SAFECOM program was brought into DHS in early 2003. In June 2003, SAFECOM partnered with the National Institute of Standards and Technology (NIST) and the National Institute of Justice (NIJ) to hold a summit that brought together over 60 entities involved with communications interoperability policy setting or programs.

Several technical factors specifically limit interoperability of public safety wireless communications systems. First, public safety agencies have been assigned frequencies in new bands over time as available frequencies become congested and as new technology made other frequencies available for use. As a result, public safety agencies now operate over multiple frequency bands—operating on these different bands required different radios because technology was not available to include all bands in one radio. Thus, the new bands provided additional capabilities but fragmented the public safety radio frequency spectrum, making communications among different jurisdictions difficult. Another technical factor inhibiting interoperability is the different technologies or different applications of the same technology by manufacturers of public safety radio equipment. One manufacturer may design equipment with proprietary technology that will not work with equipment produced by another manufacturer.

Current Status of Wireless Communications Interoperability Nationwide Is Unknown

The current status of wireless interoperable communications across the nation—including the current interoperable communications capabilities of first responders and the scope and severity of the problems that may exist—has not been determined. Although various reports have documented the lack of interoperability of public safety first responders wireless communications in specific locations, complete and current data do not exist documenting the scope and severity of the problem at the local, state, interstate, or federal levels across the nation. Accumulating this data may be difficult, however, because several problems inhibit efforts to identify and define current interoperable communications capabilities and future requirements.

First, current capabilities must be measured against a set of requirements for interoperable communications, and these requirements vary according to the characteristics of specific incidents at specific locations. Who needs

to talk to whom, when they need to talk, and what set of communications capabilities should be built or acquired to satisfy these requirements depends upon whether interoperable communications are needed for day-to-day mutual aid, task force operations that occur when members of different agencies come together to work on a common problem such as the National Capitol Region sniper investigation, or major events such as a terrorist attack. Requirements for interoperable communications also may change with the expanding definition of first responders—from the traditional police, fire, and emergency medical providers to include such professions as health care providers and other professions—and the evolution of new technology.

Establishing a national baseline for public safety wireless communications interoperability will be difficult because the definition of whom to include as a first responder is evolving, and interoperability problems and solutions are situation specific and change over time to reflect new technologies and operational requirements. SAFECOM has embarked on an effort to establish a national baseline of interoperable communications capabilities by July 2005, but SAFECOM is still working out the details of the study that would be used to develop the baseline. At the time of our review, SAFECOM officials acknowledged that establishing a baseline will be difficult and said they are working out the details of their baseline study but still expect to complete it by July 2005.

Second, technical standards for interoperable communications are still under development. Beginning in 1989, a partnership between industry and the public safety user community developed what is known as Project 25 (P-25) standards. According to the Public Safety Wireless Network (PSWN)[6] program office, Project 25 standards remain the only user-defined set of standards in the United States for public safety communications. DHS purchased radios that incorporate the P-25 standards for each of the nation's 28 urban search and rescue teams. PSWN believes P-25 is an important step toward achieving interoperability, but the standards do not mandate interoperability among all manufacturers' systems. Standards development continues today as new technologies emerge that meet changing user needs and new policy requirements.

[6]DOJ and the Department of the Treasury formed PSWN to promote effective public safety communications and to foster interoperability among local, state, federal, and tribal communications systems. PSWN was incorporated into DHS as part of the SAFECOM project in 2003.

Third, new public safety mission requirements for video, imaging, and high-speed data transfers, new and highly complex digital communications systems, and the use of commercial wireless systems are potential sources of new interoperability problems. Availability of new spectrum can also encourage the development of new technologies and require further development of technical standards. For example, the FCC recently designated a new band of spectrum, the 4.9 Gigahertz (GHz) band, for use and support of public safety. The FCC provided this additional spectrum to public safety users to support new broadband applications such as high-speed digital technologies and wireless local area networks for incident scene management. In providing the additional spectrum, the FCC requested comments on the implementation of technical standards for fixed and mobile operations on the band.

Federal Leadership Could Facilitate Interoperable Wireless Communications

The federal government, states, and local governments have important roles to play in assessing interoperability needs, identifying gaps in meeting those needs, and developing comprehensive plans for closing those gaps. The federal government can provide the leadership, long-term commitment, and focus to help state and local governments meet these goals. For example, currently national requirements for interoperable communications are incomplete and no national architecture exists, there is no standard database to coordinate frequencies, and no common nomenclature or terminology exists for interoperability channels. States alone cannot develop the requirements or a national architecture, compile the nationwide frequency database, or develop a common nationwide nomenclature. Moreover, the federal government alone can allocate communications spectrum for public safety use.

National Requirements and a National Architecture Are Needed

One key barrier to the development of a national interoperability strategy has been the lack of a statement of national mission requirements for public safety—what set of communications capabilities should be built or acquired—and a strategy to get there. A key initiative in the SAFECOM program plan for the year 2005 is to complete a comprehensive Public Safety Statement of Requirements. The Statement is to provide functional requirements that define how, when, and where public safety practitioners communicate. On April 26, 2004, DHS announced the release of the first comprehensive Statement of Requirements defining future communication requirements and outlining future technology needed to meet these requirements. According to DHS, the Statement provides a shared vision and an architectural framework for future interoperable public safety communications. DHS describes the Statement of Requirements as a living

document that will define future communications services as they change or become new requirements for public safety agencies in carrying out their missions. SAFECOM officials said additional versions of the Statement will incorporate whatever is needed to meet future needs but did not provide specific details.

A national architecture has not yet been prepared to guide the creation of interoperable communications. An explicit, commonly understood, and agreed-to blueprint, or architecture, is required to effectively and efficiently guide modernization efforts. SAFECOM officials said they are responsible for development of a national communications architecture and that will take time because SAFECOM must first assist state and local governments to establish their communications architectures. They said SAFECOM will then collect the state and local architectures and fit them into a national architecture that links federal communications into the state and local infrastructure.

Standard Databases and Common Nomenclature Have Not Been Established

Technology solutions by themselves are not sufficient to fully address communication interoperability problems in a given local government, state, or multi-state region. State and local officials consider a standard database of interoperable communications frequencies to be essential to frequency planning and coordination for interoperability frequencies and for general public safety purposes. Police and fire departments often have different concepts and doctrines on how to operate an incident command post and use interoperable communications. Similarly, first responders, such as police and fire departments, may use different terminology to describe the same thing. Differences in terminology and operating procedures can lead to communications problems even where the participating public safety agencies share common communications equipment and spectrum. State and local officials have drawn specific attention to problems caused by the lack of common terminology in naming the same interoperability frequency.

The Public Safety National Communications Council (NCC) was appointed by the FCC to make recommendations for public safety use of the 700 MHz communications spectrum. The NCC recommended that the FCC mandate

(1) Regional Planning Committee[7] use of a standard database to coordinate frequencies during license applications and (2) designation of specific names for each interoperability channel on all pubic safety bands. The NCC said that both were essential to achieve interoperability because public safety officials needed to know what interoperability channels were available and what they were called. In January 2001, the FCC rejected both recommendations. It said that the first recommendation was premature because the database had not been fully developed and tested. The FCC directed the NCC to revisit the issue of mandating the database once the database was developed and had begun operation. The FCC rejected the common nomenclature recommendation because it said that it would have to change the rules each time the public safety community wished to revise a channel label. In its final report of July 25, 2003, the NCC renewed both recommendations. It noted that the FCC had received a demonstration of a newly developed and purportedly operational database, the Computer Assisted Pre-Coordination Resource and Database System (CAPRAD), and that its recommendations were consistent with previous FCC actions, such as the FCC's designating medical communications channels for the specific purpose of uniform usage.

SAFECOM's Functions Are Critical for a Long-Term Program

In 2001, OMB established SAFECOM to unify the federal government's efforts to help coordinate work at the federal, state, local, and tribal levels in order to provide reliable public safety communications and achieve national wireless communications interoperability. However, SAFECOM was established as an OMB E-Gov initiative with a goal of improving interoperable communications within 18-24 months—a timeline too short for addressing the complex, long-term nature of the interoperability problem.[8] In addition, the roles and responsibilities of various federal

[7]In 1987, the FCC developed a National Plan for Public Safety Radio Services that set national guidelines for use of the 800 MHz spectrum while allowing regional public safety planning committees to develop regional plans tailored to their areas own particular communications needs. A large portion of the 700 MHz public safety spectrum, approximately 53 percent (12.5 MHz), is designated for general use by local, regional, and state users. A regional planning process was adopted to govern management of this public safety spectrum. It is a process similar to that used in the 821-824 MHz and 866-869 MHz bands. Regional Planning Committees (RPCs) are allowed maximum flexibility to meet state and local needs, encourage innovative use of the spectrum, and accommodate new and as yet unanticipated developments in technology equipment. They are responsible for creating and managing regional plans.

[8]U.S. General Accounting Office, *Project SAFECOM: Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration*, GAO-04-494 (Washington, D.C.: April 16, 2004).

agencies within and outside DHS involved in communications interoperability have not been fully defined, and SAFECOM's authority to oversee and coordinate federal and state efforts has been limited in part because it has been dependent upon other federal agencies for cooperation and funding and has operated without signed memorandums of understanding negotiated with various agencies.

DHS, where SAFECOM now resides, announced in May 2004 that it had created an Office for Interoperability and Compatibility within the Science and Technology Directorate, to coordinate the federal response to the problems of wireless and other functional interoperability and compatibility. The new office is responsible for coordinating DHS efforts to address interoperability and compatibility of first responder equipment, to include both communications equipment and equipment such as personal protective equipment used by police and fire from multiple jurisdictions. The plan as approved by the Secretary of DHS states that by November 2004 the new office will be fully established and that action plans and a strategy will be prepared for each portfolio (type or class of equipment). The plan presents a budget estimate for creation of the office through November 2004 but does not include costs to implement each portfolio's strategy. The plans for the new office do not clarify the roles of various federal agencies or specify what oversight authority the new office will have over federal agency communications programs. As of August 2004, the exact structure and funding for the office, including SAFECOM's role within the office, were still being developed.

Multiple Federal Agencies Have Roles And Responsibilities For Interoperability

DHS has not defined how it will convert the current short-term program and funding structures to a permanent program office structure. When it does, DHS must carefully define the SAFECOM mission and roles in relation to other agencies within DHS and in other federal agencies that have missions that may be related to the OMB-assigned mission for SAFECOM. SAFECOM must coordinate with multiple federal agencies, including ODP within DHS, the Advanced Generation of Interoperability for Law Enforcement (AGILE)[9] program and the Office for Community

[9]AGILE was the DOJ program to assist state and local law enforcement agencies to communicate effectively and efficiently with one another across agency and jurisdictional boundaries. DOJ's National Institute of Justice (NIJ) has announced it is bringing the AGILE program to a close and initiating a new program called Communications Technology, or CommTech.

Oriented Policing Services (COPS)[10] in DOJ, the Department of Defense, the FCC, NTIA within the Department of Commerce, and other agencies. The Homeland Security Act of 2002 assigns the DHS Office for Domestic Preparedness (ODP) primary responsibility within the executive branch for preparing the United States for acts of terrorism, including coordinating or, as appropriate, consolidating communications and systems of communications relating to homeland security at all levels of government. An ODP official said the Homeland Security Act granted authority to ODP to serve as the primary agency for preparedness against acts of terrorism, to specifically include communications issues. He said ODP is working with states and local jurisdictions to institutionalize a strategic planning process that assesses and funds their requirements. ODP also plans to develop tools to link these assessments to detailed interoperable communications plans.

SAFECOM officials also will face a complex issue when they address public safety spectrum management and coordination. NTIA is responsible for federal government spectrum use, and the FCC is responsible for state, local, and other nonfederal spectrum use. The National Governors' Guide to Emergency Management noted that extensive coordination will be required between the FCC and the NTIA to provide adequate spectrum and to enhance shared local, state, and federal communications. In September 2002, GAO reported that FCC and NTIA efforts to manage their respective areas of responsibility were not guided by a national spectrum strategy, and the agencies had not implemented long-standing congressional directives to conduct joint, national spectrum planning.[11] The FCC and the NTIA generally agreed with our recommendation that they develop a strategy for establishing a clearly defined national spectrum plan and submit a report to the appropriate congressional committees. In a separate report, we also discussed several barriers to reforming spectrum management in the United States.[12] On June 24, 2004, the Department of

[10]Congress authorized COPS within DOJ to administer the Interoperable Communications Technology Program in 2003. The program awarded 14 grants totaling more than $66 million to first responders for interoperable communications and provides technical assistance to grantees.

[11]U.S. General Accounting Office, *Telecommunications: Better Coordination and Enhanced Accountability Needed to Improve Spectrum Management*, GAO-02-906 (Washington, D.C.: Sept. 2002).

[12]U.S. General Accounting Office, *Telecommunications: Comprehensive Review Of U.S. Spectrum Management With Broad Stakeholder Involvement Is Needed*, GAO-03-277 (Washington, D.C.: Jan. 2003).

Commerce released two reports entitled *Spectrum Policy for the 21st Century—The President's Spectrum Policy Initiative*, the second of which contained recommendations for assessing and managing public safety spectrum.[13]

SAFECOM's Authority to Coordinate Federal and State Efforts Is Limited

SAFECOM has limited authority to coordinate federal efforts to assess and improve interoperable communications. Although SAFECOM has developed guidance for use in federal first responder grants, SAFECOM does not have authority to require federal agencies to coordinate their grant award information. SAFECOM is currently engaged in an effort with DOJ to create a "collaborative clearinghouse" that could facilitate federal oversight of interoperable communications funding to jurisdictions and allow states access to this information for planning purposes. The database is intended to decrease duplication of funding and evaluation efforts, de-conflict the application process, maximize efficiency of limited federal funding, and serve as a data collection tool for lessons learned that would be accessible to state and locals. However, SAFECOM officials said that the challenge to implementing the coordinated project is getting federal agency collaboration and compliance. As of February 2004, the database contained award information from the 2003 COPS and FEMA interoperability communications equipment grants, but no others within or outside DHS.

SAFECOM's oversight authority and responsibilities are dependant upon its overall mission. OMB officials told us that they are currently in the process of refocusing the mission of the SAFECOM program into three specific parts: (1) coordination of federal activities through several initiatives, including participation in the Federal Interagency Coordination Council (FICC)[14] and establishment of a process for federal agencies to report and coordinate with SAFECOM on federal activities and

[13]U.S. Department of Commerce, *Spectrum Policy For the 21st Century—The President's Spectrum Policy Initiative: Report 1, Recommendations Of The Federal Government Spectrum Task Force* and *Report 2, Recommendations From State and Local Governments And Private Sector Responders* (Washington, D.C.: June 2004).

[14]FICC is an informal council consisting of federal agencies, whose mission is to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications by reducing duplication in programs and activities, identifying and promoting best practices, and coordinating federal grants, technical assistance, training, and standards. Proposed FICC members are federal agencies within DOJ, DHS, Defense, Agriculture, Health and Human Services, and Commerce.

investments in interoperability; (2) developing standards; and (3) developing a national architecture for addressing communications interoperability problems. They said identification of all current and planned federal agency communications programs affecting federal, state, and local wireless interoperability is difficult. According to these officials, OMB is developing a strategy to best utilize the SAFECOM program and examining options to enforce the new coordination and reporting process. SAFECOM officials said they are working to formalize the new reporting and coordination process by developing written agreements with other federal agencies and by obtaining concurrence of major state and local associations to the SAFECOM governance structure. SAFECOM officials noted that this newly refocused SAFECOM role does not include providing technical assistance or conducting operational testing of equipment. They said that their authority to conduct such activities would come from DHS enabling directives. SAFECOM officials also said that they have no enforcement authority to require other agencies to use the SAFECOM grant guidance in their funding decisions or to require agencies to provide grant program information to them for use in their database.

State and Local Governments Can Play a Central Role

States, with broad input from local governments, can serve as focal points for statewide planning to improve interoperable communications. The FCC has recognized the important role of states. In its rules and procedures, the FCC concluded that because states play a central role in managing emergency communications and are usually in control at large scale-events and disasters, states should administer the interoperability channels within the 700 MHz band of communications spectrum. States can play a key role in improving interoperable communications by establishing a management structure that includes local participation and input to analyze and identify interoperability gaps between "what is" and "what should be," developing comprehensive local, state, and regional plans to address such gaps, and funding implementation of these plans. The states we visited or contacted—California, Florida, Georgia, Missouri, Washington and a five-state Midwest consortium—were in various stages of formulating these management structures.

States are not required to establish a statewide management structure or to develop interoperability plans, and there is no clear guidance on what should be included in such plans. In addition, no requirement exists that interoperability of federal communications systems be coordinated with state and local government communications systems. The use of a standard database on communications frequencies by public safety agencies within the state and common terminology for these frequencies

in preparation and implementation of these statewide interoperable plans are essential but are also not required. Without planning, coordination, and applicable standards, the communications systems developed between and among locations and levels of government might not be interoperable.

States are key players in responding to normal all-hazards emergencies and to terrorist threats. Homeland Security Presidential Directive 8 notes that awards to states are the primary mechanism for delivery of federal preparedness assistance for these missions. State and local officials also believe that states, with broad local and regional participation, have a key role to play in coordinating interoperable communications supporting these missions. The Public Safety Wireless Network (PSWN), in its report on the role of the state in providing interoperable communications, agreed. According to the PSWN report, state leadership in public safety communications is key to outreach efforts that emphasize development of common approaches to regional and statewide interoperability. The report said that state officials have a vested interest in establishing and protecting statewide wireless infrastructures because public safety communications often must cross more than one local jurisdictional boundary.[15]

However, states are not required to establish a statewide capability to (1) integrate statewide and regional interoperability planning and (2) prepare statewide interoperability plans that maximize use of spectrum to meet interoperability requirements of day-to-day operations, joint task force operations, and operations in major events. Federal, state, and local officials are not required to coordinate federal, state, and local interoperability spectrum resources that, if successfully addressed, have significant potential to improve public safety wireless communications interoperability. As a result, states may not prepare comprehensive and integrated statewide plans that address the specific interoperability issues present in each state across first responder disciplines and levels of government.

Federal interoperability with state and local wireless communications systems is hindered because NTIA and FCC control different frequencies in the VHF and UHF bands. To enhance interoperability, NTIA has identified 40 federal government frequencies that can be used by state and local public safety agencies for joint law enforcement and incident

[15]See *The Role of The States in Public Safety Wireless Interoperability*, PSWN (2002).

response purposes.[16] FCC, however, designated different frequencies for interoperability in the VHF band and in the UHF band from spectrum it controls for use by state and local public safety agencies.

Federal Grant Structure Does Not Support Statewide Planning

DHS recently estimated that reaching an accelerated goal of communications interoperability will require a major investment of several billion dollars within the next 5 to 10 years. As a result of these extraordinary costs, federal funding is but one of several resources state and local agencies must use in order to address these costs. Furthermore, given the high costs, the development of an interoperable communications plan is vital to useful, non-duplicative spending. However, the federal funding assistance programs to state and local governments do not fully support regional planning for communications interoperability. Federal grants that support interoperability have different requirements to tie funding to interoperable communications plans. In addition, uncoordinated federal and state level grant reviews limit the government's ability to ensure that federal funds are used to effectively support improved regional and statewide communications systems.

States and Local Governments Are Not Required to Provide Interoperable Communications Plans

Local, state and federal officials agree that regional communications plans should be developed to guide decisions on how to use federal funds for interoperable communications; however, the current funding requirements do not support this planning process. Although recent grant requirements have encouraged jurisdictions to take a regional approach to planning, current federal first responder grants differ in their requirements to tie funding to interoperable communications plans. State and local jurisdictions are not required to provide an interoperable communications plan as a prerequisite to receiving some federal grant funds. As a result, there is no assurance that federal funds are being used to support a well-developed strategy for improving interoperability. For example, the fiscal year 2004 Homeland Security Grants and Urban Areas Security Initiative (UASI) grants require new grantees to conduct a needs assessment and submit a Homeland Security Strategy to ODP, and continuation grantees to allocate funds according to their existing Homeland Security Strategies. However, the required strategies are high-level and broad in nature. They

[16]NTIA states that these frequencies may not be used to meet day-to-day communications needs of non-federal public safety agencies.

do not require that project narratives or a detailed communications plan be submitted by grantees prior to receiving grant funds.

In another example, fiscal year 2003 funding provided by COPS and FEMA for the Interoperable Communications Equipment Grants did not require that a communications plan be completed prior to receiving grant funds. However, grantees were required to provide documentation that they were actively engaged in a planning process and a multi-jurisdictional and multidisciplinary project narrative was required. In addition to variations in requirements to create communications interoperability plans, federal grants also lack consistency in defining what "regional" body should conduct planning.

Grant Submissions and Performance Period Time Frames Also Present Challenges to Short- and Long-Term Planning

State and local officials also said that the short grant application deadlines for recent first responder grants limited their ability to develop cohesive communications plans or perform a coordinated review of local requests. Federal officials acknowledged that the limited submission timeframes present barriers to first responders for developing plans prior to receiving funds. For example, several federal grant programs—the Homeland Security Grants, UASI grants, COPS and FEMA interoperable communication equipment grants, and Assistance to Firefighters Grants—allow states only 30 or 60 days from the date of grant announcement to submit a grant proposal. These time frames are sometimes driven by appropriations language or by the timing of the appropriations enactment. Furthermore, many grants have been awarded to state and locals for communications interoperability that have 1 or 2 year performance periods, and according to state and local officials, do not support long-term solutions. For example, Assistance to Fire Fighters Grants, COPS/FEMA's interoperable communications equipment grants, and National Urban Search and Rescue grants all have 1-year performance periods.[17] UASI, the Homeland Security Grants program, and DOJ's Local Law Enforcement Block Grants have 2-year performance periods.

[17]COPS officials said that although the performance period for the FY 2003 Interoperable Communications Technology Equipment and the COPS Interoperable Communications Technology Program was one year, no-cost extensions of time were available to grantees on a case-by-case basis to accommodate unavoidable delays.

No Coordinated Federal or State Grant Review Exists to Ensure Funds are Used to Improve Regional or Statewide Communications Interoperability

The federal and state governments lack a coordinated grant review process to ensure that funds allocated to local governments are used for communication projects that complement each other and add to overall statewide and national interoperability. Federal and state officials said that each agency reviews its own set of applications and projects, without coordination with other agencies. As a result, grants could be given to bordering jurisdictions that propose conflicting interoperability solutions. In fiscal year 2003, federal officials from COPS and FEMA attempted to eliminate awarding funds to conflicting communication systems within bordering jurisdictions by coordinating their review of interoperable communications equipment grant proposals. However, COPS and FEMA are only two of several federal sources of funds for communications interoperability.

In an attempt to address this challenge, in 2003, SAFECOM coordinated with other agencies to create the document, *Recommended Federal Grant Guidance, Public Safety Communications and Interoperability Grants*, which lays out standard grant requirements for planning, building, and training for interoperable communications systems. The guidance is designed to advise federal agencies on who is eligible for the first responder interoperable communications grants, the purposes for which grant funds can be used, and eligibility specifications for applicants.[18] The guidance recommends standard minimum requirements, such as requirements to "...define the objectives of what the applicant is ultimately trying to accomplish and how the proposed project would fit into an overall effort to increase interoperability, as well as identify potential partnerships for agreements." Additionally, the guidance recommends, but does not require, that applicants establish a governance group consisting of local, tribal, state, and federal entities from relevant public safety disciplines and purchase interoperable equipment that is compliant with phase one of Project-25 standards.

Conclusions

A fundamental barrier to successfully addressing interoperable communications problems for public safety has been the lack of effective, collaborative, interdisciplinary, and intergovernmental planning.

[18]DHS officials said that, in addition to outlining the eligibility for grant dollars and the purposes for which federal dollars can be used, the SAFECOM grant guidance provides consensus guidelines for implementing a wireless communications system. DHS said this guidance is useful in directing all agencies towards interoperability goals, even if they are not specifically applying for federal funding.

Jurisdictional boundaries and unique public safety agency missions have often fostered barriers that hinder cooperation and collaboration. No one first responder agency, jurisdiction, or level of government can "fix" the nation's interoperability problems, which vary across the nation and often cross first responder agency and jurisdictional boundaries. Changes in spectrum available to federal, state and local public safety agencies—primarily a federal responsibility conducted through the FCC and NTIA—changes in technology, and the evolving missions and responsibilities of public safety agencies in an age of terrorism all highlight the ever-changing environment in which interoperable communications needs and solutions must be addressed and effective federal leadership provided. Interdisciplinary, intergovernmental, and multi-jurisdictional partnership and collaboration are essential for effectively addressing interoperability shortcomings.

Recommendations

In our July 2004 report,[19] we made recommendations to DHS and OMB to improve the assessment and coordination of interoperable communications efforts. We recommended that the Secretary of DHS:

- in coordination with the FCC and NTIA, continue to develop a nationwide database of public safety frequency channels and a standard nationwide nomenclature for these channels, with clear target dates for completing both efforts;
- establish requirements for interoperable communications and assist states in assessing interoperability in their states against those requirements;
- through DHS grant guidance encourage states to establish a single, statewide body to assess interoperability and develop a comprehensive statewide interoperability plan for federal, state, and local communications systems in all frequency bands; and
- at the appropriate time, require through DHS grant guidance that federal grant funding for communications equipment be approved only upon certification by the statewide body responsible for interoperable communications that grant applications for equipment purchases conform with statewide interoperability plans.

[19]U.S. Government Accountability Office, *Homeland Security: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications*, GAO-04-740 (Washington, D.C.: July 2004).

We also recommended that the Director of OMB, in conjunction with DHS, review the interoperability mission and functions now assigned to SAFECOM and establish those functions as a long-term program with adequate authority and funding.

In commenting on our July 2004 report, the Department of Homeland Security discussed actions the department is taking that are generally consistent with the intent of our recommendations but did not directly address specific steps detailed in our recommendations with respect to establishment of statewide bodies responsible for interoperable communications within the state, the development of comprehensive statewide interoperability plans, and tying federal funds for communications equipment directly to those statewide interoperable plans. OMB did not provide written comments on the draft report.

This concludes my prepared statement, Mr. Chairman. I would be pleased to answer any questions you or other members of the Subcommittee may have at this time.

GAO Contacts and Acknowledgments

For future contacts regarding this testimony, please call William O. Jenkins, Jr., Homeland Security and Justice Issues, at (202) 512-8777. Other individuals who made key contributions to this testimony include Katherine Davis, Sally Gilley, Robert Hadley, Latesha Love, Gary Malavenda, and Thomas James.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov(202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER

Mr. PUTNAM. Thank you very much, Mr. Jenkins.

Our next witness is Dr. David Boyd. Dr. Boyd is the Deputy Director of System Engineering and Development under DHS' Science and Technology Directorate. He serves as the Director of the Project SAFECOM program office, and was recently placed in charge of creating the Department's new Office of Interoperability and Compatibility. He is also a member of the President's National Task Force on Spectrum Management.

Prior to his work on the civilian side, Dr. Boyd served in the U.S. Army for more than 20 years, in which he commanded combat, combat support and training units in both war and peace, and has served on military staffs from battalion level to the Pentagon. He has more than three dozen military awards, including the Bronze Star and the Purple Heart.

Dr. Boyd holds a career appointment in the Senior Executive Service, is a graduate of the University of Illinois and holds graduate degrees in operations research and public policy analysis, as well as a doctorate in decision sciences. He is widely published and we are delighted to have him. Dr. Boyd, you are recognized for 5 minutes.

STATEMENT OF DAVID G. BOYD, PH.D., DIRECTOR, SAFECOM PROGRAM OFFICE, SCIENCE AND TECHNOLOGY DIRECTORATE, DEPARTMENT OF HOMELAND SECURITY

Mr. BOYD. Thank you, Mr. Chairman, members of the subcommittee. Thank you for the invitation to testify before you today.

Mr. Chairman, as you, Chairman Davis and Chairman Shays observed recently in a letter to GAO, "Effective communications between and among wireless communications systems used by Federal, State and local public safety agencies is generally accepted as not only desirable, but essential for the protection of life and property."

Interoperability is not a new issue for public safety. It was a problem in 1984 when the Air Florida flight crashed into the Potomac; in New York City when the Twin Towers were bombed in 1993; at the Murrah Building in Oklahoma City; at Columbine and on September 11. But September 11 put the issue in such stark relief that more effort has now gone into interoperability than at any time in history.

Since 2001, FEMA and the COPS office have partnered with SAFECOM to coordinate well over $230 million in interoperability grants to localities. At least $1.1 billion more has been provided through preparedness grants to States. Two major interoperability initiatives have been or are being established at the highest levels: SAFECOM, established as a Presidential Management Initiative, and the DHS effort to establish an Office of Interoperability and Compatibility by the end of this year.

When I testified before you last November, interoperability programs were spread across the Government. The Homeland Security Act had made three different agencies responsible for interoperability in DHS alone: the Office of Domestic Preparedness, the Federal Emergency Management Agency, and even an agency in the Department of Justice. SAFECOM was under its fourth program

manager and the Government Accountability Office was finishing one study of the program and beginning another.

I'm happy to report to you today that while much remains to be done, and responsibility for interoperability remains diffused across the Government, our efforts to bring order to the problem have been validated by the most recent GAO report and by the major State and local public safety associations, who declared in January that "with the advent of the SAFECOM Program public safety, and State and local government finally have both a voice in public safety discussions at the Federal level and confidence that the Government is coordinating its resources."

We have created the Federal Interagency Coordinating Council to coordinate funding, technical assistance, standards development and regulations affecting communications and interoperability across the Federal Government. We have published a statement of requirements which, for the first time, defines what it will take to achieve full interoperability and provides industry requirements against which to map their product capabilities. We have issued a request for proposals for the development of a national interoperability baseline and will make an award in October.

We have issued a request for information to industry to tell us what technologies they had or were developing to help with interoperability which produced more than 150 responses. We have accelerated the development of critical standards for interoperability and developed a framework for defining a national architecture.

We have created coordinated grant guidance and implemented it in the FEMA and COPS interoperability grants last year, and in the COPS interoperability grants and ODP State block grants this year. We have established a joint task force with the FEDERAL Communications Commission to consider spectrum and regulatory issues that affect interoperability. And we've created a model methodology with the State of Virginia for the development of statewide communications plans supported at every level within the State.

Since we know neither terrorists nor natural disasters will wait, the Secretary has directed the Science and Technology Directorate to provide assistance to 10 high threat urban areas through a program called RAPIDCom. We found that most of the 10 urban areas have the technical capability to achieve a basic command level of interoperability, but lack many of the operational elements required to actually achieve interoperability, so that, in some cases, equipment provided by the Federal Government is still not integrated into the local system. We have been working for several months now to help fill those operational gaps, since technology, as our interoperability continuum displayed on the easel before you illustrates, is only one of the elements needed for successful interoperability.

Earlier this year, the Secretary of DHS directed the Science and Technology Directorate to establish a new Office of Interoperability and Compatibility to address relevant equipment and training as well as communications. We have already identified more than 60 different programs in the Federal Government that deliver equipment or training to first responders.

We still have much to do, but we have laid a firm foundation. Never before has a Presidential Management Initiative existed that

addresses communications interoperability issues at all levels of Government. Never before has Congress made so much grant money available for States and localities to improve their interoperability.

Never before has common grant guidance been applied across the entire Federal Government. Never before has a national statement of requirements for interoperability existed.

We are confident that with your continuing support and the assistance of our many local, State and Federal partners, we can ensure that lives and property are never lost because public safety agencies cannot communicate. Thank you, Mr. Chairman.

[The prepared statement of Mr. Boyd follows:]

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 Technology, Information Policy, Intergovernmental Relations and the Census

September 8, 2004

Table of Contents

Introduction 3
SAFECOM Background 4
The Creation of Architectural Framework 5
The Development of Standards 6
Federal Coordination 6
Near- term Solutions 7
Practitioner Driven Philosophy 8
Conclusion 9

Introduction

On September 11, 2001, thousands of American citizens died at the hands of terrorists. The tragic events of that day clarified the critical importance of effective first responder communication systems. As Chairman Putnam, in company with Chairman Davis and Chairman Shays observed recently,

> The inability of first responders – police officers, fire fighters, emergency medical service personnel, public health officials, and others – to communicate effectively over wireless systems with one another as needed during an emergency is a long-standing and widely recognized problem in many areas across the country. Reports have shown that when first responders cannot communicate effectively as needed, it can literally cost lives of both emergency responders and those they are trying to assist. Thus, effective communications between and among wireless communications systems used by Federal, State, and local public safety agencies is generally accepted as not only desirable but essential for the protection of life and property.[1]

The Government Accountability Office (GAO), at the direction of Chairmen Davis, Shays, and Putnam, recently completed an examination of the interoperability problem. We are heartened that the GAO report validates our efforts, activities, strategic plan, and overall guiding philosophy.

Today's testimony will focus on the Department of Homeland Security (DHS) efforts to improve communications interoperability in both the near and long-term for public safety first responders, SAFECOM, managed by the Science and Technology Directorate. Much of SAFECOM's efforts are focused on long-term strategic initiatives without which the nation will never solve the interoperability problem. However, the Secretary of DHS has directed that SAFECOM also undertake measures to achieve immediate interoperability sufficient to meet the most likely near-term emergencies. We will also discuss DHS' efforts to develop and launch the Office for Interoperability and Compatibility (OIC), which will build on the SAFECOM model to address interoperability needs related to training and equipment as well as to communications.

As noted in the GAO report , "Public safety agencies have historically planned and acquired communications systems for their own jurisdictions without concern for interoperability."[2] The story is not dramatically different for Federal wireless systems, so SAFECOM was created to help bring order to the nation's public safety wireless communications systems at all levels of government. More importantly, it provides a single coordinating point for the country, since many agencies have either been directed by Congress – in response to the tragic experiences of 9/11 – to address interoperability, or have taken it upon themselves to do so. Under the Homeland Security Act, for example, three DHS' entities are charged with addressing interoperability. The Office of Domestic Preparedness is charged with "coordinating or, as appropriate, consolidating communications and systems of communications relating to homeland security at all levels of government."[3] Section 502 (7) of the same act charges the Emergency

---

[1] Government Accountability Office (GAO), (July, 2004), *HOMELAND SECURITY: Federal Leadership and Intergovernmental Cooperation Required to Achieve First Responder Interoperable Communications, p. 1.*
[2] GAO, (July 2004), p. 9.
[3] Section 430 (c) (2).

Preparedness and Response Directorate with "developing comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology." Section 232 (b) (7), again of the same Act, directs an agency of the Department of Justice to "administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications." In late May, 2003, in cooperation with the Commerce and Justice Departments, we assembled representatives from 60 different programs either inside the Federal Government, or funded by or partnered with a Federal agency, all of which touched in some way on interoperability. By coordinating and leveraging the vast range of interoperability programs and related efforts spread across the Federal Government, SAFECOM is reducing unnecessary duplication of programs and spending and ensuring consistency across Federal activities related to research and development, testing and evaluation (RDT&E), standards, technical assistance, training, and grant funding related to interoperability. The new Office for Interoperability and Compatibility will do the same across the Department of Homeland Security. Much as has SAFECOM, OIC will face significant challenges, but we are confident that with the high level of Executive and Congressional support we have enjoyed to date, and the support of local, state, and Federal partners, we will continue to see extensive improvements in public safety interoperability.

SAFECOM Background

Interoperability is not a new issue; it has plagued the public safety community for decades. It was a problem in Washington, D.C., when the Air Florida flight crashed into the Potomac River. It was a problem in New York City when the Twin Towers were first attacked in 1993. It was a problem when the Murrah Building was destroyed in Oklahoma City, and finally, interoperability was an issue in the Columbine school shooting spree. The reality is that today, too many agencies cannot communicate by radio because their equipment is still incompatible, or the frequencies they are assigned are different. They operate on numerous frequency bands and run communications systems which are often 30 years old, in an era when the technology lifecycle is only 18 to 24 months. But national efforts to fix the problem, one which had long vexed public safety, were erratic, uncertain, and uncoordinated. With the attacks on September 11, 2001, we recognized we must take a more aggressive approach to correct the problem.

Since 2001, more effort has gone into solving the interoperability problem than at any other time in history. DHS' Federal Emergency Management Agency (FEMA) and the Department of Justice's Community Oriented Policing Services (COPS) office have partnered to coordinate more than $230 million appropriated by Congress for grants specifically to address interoperability. Additionally more than $1.1 billion has been provided in grants to states for use for a variety of preparedness initiatives, including interoperability. Two major interoperability initiatives – for the first time in the nation's history – have been or are being established at the highest levels to solve the interoperability problem: SAFECOM two years ago as a Presidential E-Gov Management Initiative (and a DHS responsibility since the summer of 2003), and the Office for Interoperability and Compatibility within the Science and Technology Directorate of the Department of Homeland Security, to be stood up officially this year.

The foundation of the SAFECOM Program and the driving force behind its success has been the support of local, state, and Federal public safety practitioners. For the first time there are new and invigorated partnerships among local, state, and Federal public safety practitioners and

agencies. SAFECOM firmly believes that any effort to improve communication interoperability must be driven from the bottom up. The involvement of public safety practitioners ensures that solutions are realistic and can actually be implemented.

Communications interoperability refers to 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. Unfortunately, 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 by SAFECOM to incorporate the needs of local, state, and Federal practitioners. However, there remain many challenges, both technical and cultural, facing the improvement of public safety communications and interoperability. As the Government Accountability Office (GAO) acknowledged in its July 2004 report, communications interoperability is a long-term problem with no one-size-fits-all solution.

SAFECOM's mission is to serve as the umbrella program within the Federal Government to help local, tribal, state, and Federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications. SAFECOM has focused on three key areas: the creation of an Architectural Framework, the development of standards, and the coordination of federal activities. Over the last year, SAFECOM has made significant progress in achieving both its short-term goals as well as building the foundation for a longer term, comprehensive interoperability program.

The Creation of Architectural Framework

The creation of an architectural framework is the foundation of the SAFECOM long-term strategic plan for improving communications interoperability. As GAO recognized, "[o]ne key barrier to the development of a national interoperability strategy has been the lack of a statement of national mission requirements for public safety – what set of communications capabilities should be built or acquired – and a strategy to get there."[4] .

SAFECOM's architectural framework, the first version of which we expect to publish in the third quarter of FY 2005, will determine priorities for the development of standards, is driven by the Statement of Requirements, and will encompass successful techniques used by local, State, regional, or Federal integration networks. This framework will reflect a system-of-systems approach to develop interface standards to help improve the problem of communications interoperability.

Although the architectural framework is a long-term goal, SAFECOM is working aggressively, partnering with key local, State, and Federal public safety practitioners, to complete the first steps in the architectural framework process. The SAFECOM Statement of Requirements (SoR) version 1.0 was completed and released in March of 2004. We have also initiated efforts to develop an accurate assessment of the current baseline of public safety communications interoperability, which is essential to understanding where the nation is now and in measuring our progress over the life of the Program. A Request for Proposals (RFP) was released several weeks ago and proposals were due in yesterday, September 7, 2004. Work on the baseline is

[4] GAO, (July, 2004), p. 53.

expected to begin not later than the first quarter of FY 2005 and will be completed as quickly as possible. Once the architectural framework is completed, it will then be possible to conduct a gap analysis to determine what will be required to move us from where we are now to a state which meets the requirements identified in the SoR.

The Development of Standards

As part of its long-term strategy for improving communications interoperability, SAFECOM will closely coordinate the development of interoperability standards with the DHS Standards Executive, in partnership with local, State, and Federal public safety organizations to define the requirements for first responder interoperability at all levels. Both SAFECOM and GAO are in strong agreement that standards are a key element of the long-term solution to interoperability. SAFECOM, building upon the SoR developed earlier this year and the Architectural Framework discussed above, will support ongoing efforts or, when necessary, initiate the creation of standards to address gaps where identified. SAFECOM efforts, and OIC once established, will draw on existing institutions such as the National Institute for Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) and will build on ongoing efforts such as the P25 standards cited by the GAO report.[5]

Federal Coordination

As the umbrella program in the Federal Government with the mission to coordinate Federal activities related to communications interoperability, the SAFECOM Program has established the Federal Interoperability Coordination Council (FICC), made up of all the Federal agencies with programs that address interoperability. Members of the FICC include those agencies that provide grants to state and local agencies (such as DHS and the Department of Justice), those that need to interoperate with each other or with state and local agencies (e.g., DHS, Justice, Agriculture, Interior, Defense and others), and standards-making and regulatory organizations (e.g., the Federal Communications Commission and the National Institute for Standards and Technology).

GAO recognized the need for an entity responsible for the coordination of various Federal programs related to interoperability and has emphasized the importance of establishing Memorandums of Understanding (MOUs) by SAFECOM with its Federal partners. The Program now has ten MOUs signed (United States Department of Agriculture, Department of Energy, Department of Defense, Department of Justice, Health and Human Services, Department of Homeland Security, National Institute of Justice, Community Oriented Policing Services, National Institute of Science and Technology, Office for Domestic Preparedness), up from one at the time of the last GAO report. In addition, SAFECOM has created charters with its various committees and partners for those cases where partners (particularly state and local partners) may see formal MOUs as burdensome bureaucratic documents.

The creation of common grant guidance is another step SAFECOM has taken to coordinate Federal efforts related to interoperability. With input from the public safety community, SAFECOM has created a coordinated grant guidance which outlines eligibility for grants, the

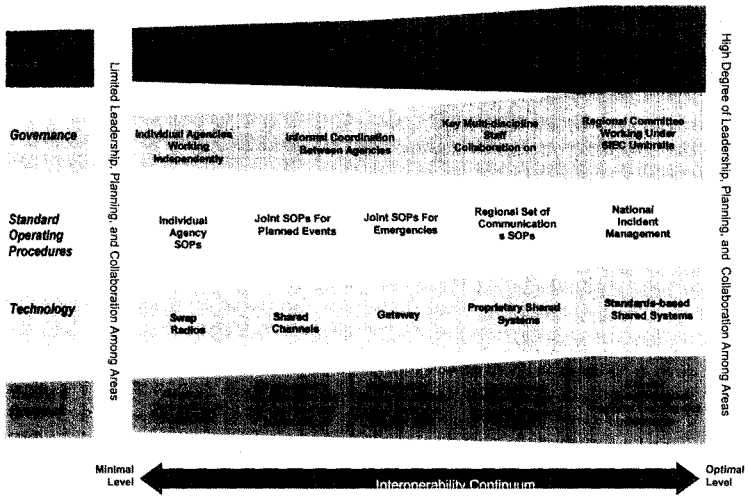
[5] P25 refers to the suite of standards under development and led by the Association of Public Safety Communications Officers (APCO).

purposes for which grants may be used in support of interoperability, and guidelines for implementing a wireless communication system. This guidance was included as part of the COPS and FEMA grants in FY 2003 and was incorporated into the COPS Interoperability grants and Office for State and Local Government Coordination and Preparedness (OSLGCP) state grants in FY 2004. Grant guidance is an important step toward in improving national interoperability because it helps to align public safety communications related grant dollars with the national effort to improve interoperability at all levels of government.

Near- term Solutions

While solving the nation's interoperability problem will take a long time, we recognize that we must ensure sufficient interoperability at all levels of government to meet emergencies of any kind, and we need to do it quickly. Begun by Secretary Ridge in early 2004, the RapidCom Initiative is providing assistance to 10 urban areas to strengthen their ability to respond to immediate emergencies. This effort is also serving as the catalyst for these areas to begin to institutionalize routine training and exercises, governance meetings, standard operating procedures, and more frequent use of interoperable communications in non-emergency situations, in order to better prepare themselves for emergencies. By working with public safety practitioners at the local level, SAFECOM is seeking to develop effective solutions to improve public safety communications and interoperability.

Fixing interoperability requires more than just the introduction of technologies. We have developed an "Interoperability Continuum" to illustrate the elements required to achieve interoperability. We believe that progression along the elements of the continuum is a parallel process, and that technology is only one of the elements. In other words, to gain a true picture of an area's interoperability, progression along all elements of the continuum must be considered. For example, if an urban area procures new equipment but has not conducted exercises to test procedures, concepts of operation, and polices, that urban area may not be fully prepared to make the best use of the new equipment. Worse, they may not recognize how little they are prepared to make use of the equipment.



Another near-term effort involves the SAFECOM's work with the Commonwealth of Virginia to develop a strategic plan for statewide communications and interoperability. The methodology we used will be provided to any state or region as a model for how to develop a successful strategic plan for interoperability. We do not believe it is possible to develop a successful statewide plan – or a national strategy – without genuine buy-in from local agencies.

Practitioner Driven Philosophy

Over ninety percent of the nation's public safety communications infrastructure is owned by localities and states. For that reason, as SAFECOM partners with other Federal agencies, we ensure that the program remains one designed by public safety for public safety and that it is based on creating interoperability solutions driven from the bottom up. The Federal Government, through the SAFECOM Program, has gained the support of all the major associations representing public safety officials (law enforcement and fire), State and local elected and appointed officials and public safety communicators. In January 2004, ten key public safety associations[6] released a joint statement that declared "With the advent of the SAFECOM

[6] Association Of Public-Safety Communications Officials – International (APCO)
International Association Of Fire Chiefs (IAFC)
International Association Of Chiefs Of Police (IACP)
Major Cities Chiefs Association (MCC)
National Sheriffs' Association (NSA)
Major County Sheriffs' Association (MCSA)
National Association Of Counties (NACO)
National League Of Cities (NLC)

Program . . . public safety, state and local government finally have both a voice in public safety discussions at the federal level and confidence that the government is coordinating its resources."

Conclusion

Over the last year, under DHS guidance, SAFECOM has made significant progress both in achieving its short-term goals and in building a foundation for a comprehensive longer term program. With strong executive and congressional support, it has established itself as the umbrella program within the Federal Government for coordination with local, State, and Federal public safety agencies to improve communications and interoperability. More importantly, it has been a catalyst for other interoperability groups and programs, and for new industry efforts to address public safety communications needs.

Our nation is heavily invested in an existing infrastructure that is largely incompatible. We must continue to pursue the current comprehensive strategy that takes into account technical and organizational issues associated with improving interoperability, and recognizes the challenges associated with incorporating legacy equipment and practices given the constantly changing nature of technology and cultural environments. Though many challenges remain, we believe we have accomplished a great deal in the short time DHS has managed the program.

Never before has there been a Presidential Management Initiative that addresses communications interoperability issues.

Never before has Congress made so much grant funding available for states and localities to improve their interoperability.

Never before has common grant guidance been applied across the entire Federal government.

Never before has a common national definition – a Statement of Requirements – developed by the nation's first responders existed to help guide public safety agencies and industry.

We are confident that with your continuing support and the assistance of our many Federal partners, we will continue to work towards a world where lives and property are never lost because public safety agencies are unable to communicate.

National Public Safety Telecommunications Council (NPSTC)
United States Conference Of Mayors (USCM)

Mr. PUTNAM. Thank you very much, Dr. Boyd.

Our next witness is Timothy Beres. Welcome to the subcommittee, Mr. Beres. Mr. Beres is the Associate Director of DHS' Office of Domestic Preparedness, with responsibility for the State and Local Operations Division. He has been with ODP since its inception.

During his tenure at the Office of Domestic Preparedness, Mr. Beres led the effort to establish the Center for Domestic Preparedness, an emergency responder training center, for the management and remediation of incidents of domestic terrorism involving chemical weapons. Additionally, he was responsible for developing ODP's national training program, developing ODP's assessment and strategy development process, and developing and implementing the pre-positioned equipment program.

Mr. Beres received his bachelor's degree from Virginia PolyTech and State University in 1991. Welcome to the subcommittee. You're recognized for 5 minutes.

STATEMENT OF TIMOTHY L. BERES, ASSOCIATE DIRECTOR, OFFICE FOR DOMESTIC PREPAREDNESS, DEPARTMENT OF HOMELAND SECURITY

Mr. BERES. Thank you, Mr. Chairman, members of the committee. It is with great pleasure that I come and speak to you today. Thank you very much for having me.

As you know, the Secretary recently established the Office of State and Local Government Coordination and Preparedness, of which ODP is now a key component. On behalf of our executive director, Suzanne Mencer, and Secretary Ridge, it is my pleasure to appear before you today to discuss briefly the current status of our program, specifically our work on interoperable communications.

The Office of Domestic Preparedness is responsible for preparing our Nation against terrorism by assisting States, local jurisdictions, regional authorities and tribal governments to prevent, respond to and recover from acts of terrorism. Through its programs and activities, ODP equips, trains, exercises and supports State and local homeland security personnel, our Nation's first responders.

During fiscal year 2004, ODP's record of service to the Nation's first responders continues. All the 56 States and territories have been awarded their fiscal year 2004 funds. These awards represent $2.2 billion in direct assistance. ODP's two primary sources for assistance to States and local communities requires them to assess their risks, capabilities and needs, which includes requirements relating to interoperable communications. Since 2002, $1.2 billion in grant assistance has been used by States and local jurisdictions to improve interoperability.

On December 17, 2003, the President issued Homeland Security Presidential Directive 8, or HSPD–8. Through this HSPD–8, the President tasked Secretary Ridge, in coordination with other Federal departments as well as State and local jurisdictions, to develop a national preparedness goal and readiness matrix to improve the delivery of Federal preparedness assistance. ODP is leading that effort for the Department.

ODP has developed and is currently implementing the Interoperable Communications Technical Assistance Program, or ICTAP.

ICTAP provides onsite technical assistance and training at no cost to first responders in conjunction with communications equipment purchased with grant funding. The program is not limited to a set time period, but focuses on quickly and thoroughly meeting unique interoperability needs and requirements of jurisdictions across the country.

The ICTAP technical assistance team works closely with the Sates and regions to provide onsite support from an initial assessment and inventory of what currently exists to live operation of the new system. This process covers four phrases: identifying requirements, identifying an appropriate solution, implementing the solution and followup and transitioning to the new system. ICTAP has received requests for assistance from 32 of the 51 participating urban area security initiative jurisdictions as well as 8 States and 3 U.S. territories.

With regard to some specific examples of work we're conducting, in South Florida significant attention is focused on the difficult policy issues of developing standard operating procedures and mutual aid agreements to address incompatible systems in that region's largest jurisdictions. In Central Florida, the immediate issue that we're working on with that region is to document what equipment is placed throughout the region. In Kansas City, Missouri, ICTAP is working with an organization called the Mid-American Regional Council, which represents city and county governments on regional issues. Working with the MARC representatives, ICTAP has proposed an interoperability solution known as the Regional Area Multi-Band Integrated System, which is a radio system that will provide interoperability between disparate radio systems.

As we are well aware, there are a number of different activities both within the Department of Homeland Security as well as with other departments that involve interoperable communications issues. As you will hear about these activities from other witnesses, I will simply state that the role of ICTAP is to fill the operational communications needs of States and regions by responding to the requests coordinated through the States. ODP looks to SAFECOM to provide standards and conduct research that can help our jurisdictions develop a better interoperable communications program. As an example, earlier this year, we adopted the SAFECOM-developed Guidelines for Interoperability as recommendations for use of funds. In addition, ODP supports Project RAPIDCom with technical experts and is a member of the Federal Interagency Coordinating Council which seeks to avoid duplication.

In closing, DHS' mission in the area of improved interoperable communications among first responders is critical. ODP fully recognizes the specific and vital role we must play. We will strive to fulfill our mission and meet our responsibilities in an effective and efficient manner. We will, to the best of our abilities, continue to identify where and how we can improve. This concludes my statement, and I am happy to respond to any questions the committee might have.

[The prepared statement of Mr. Beres follows:]

Statement

of

Timothy L. Beres

Associate Director

Office for Domestic Preparedness

before

the

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

United States House of Representatives

September 8, 2004

Washington, D.C.

Chairman Putnam, Members of the Committee, my name is Tim Beres, and I serve as the Associate Director of the Department of Homeland Security's (DHS) Office for Domestic Preparedness (ODP). As you know, the Secretary recently consolidated ODP and the Office of State and Local Government Coordination to establish the Office of State and Local Government Coordination and Preparedness (SLGCP) to move toward the "one stop shop" that State and local stakeholders have long called for. On behalf of SLGCP, Executive Director C. Suzanne Mencer, and Secretary Ridge, it is my pleasure to appear before you today to discuss the current status of SLGCP and specifically our work on interoperable communications.

On behalf of all of us at DHS, I want to thank all the Members of the Committee for your ongoing support of the Department and for SLGCP. I also want to thank you, Mr. Chairman, for your foresight and leadership on the issue of interoperable communications, which is a cornerstone of our ability to prevent and respond to acts of terrorism here in the United States.

OFFICE FOR DOMESTIC PREPAREDNESS

As you are all aware, ODP within SLGCP is responsible for preparing our Nation against terrorism by assisting States, local jurisdictions, regional authorities, and tribal governments with building their capacity to prevent, respond to, and recover from acts of terrorism. Through its programs and activities, ODP equips, trains, exercises, and supports State, local, and tribal homeland security

personnel -- our Nation's first responders -- who may be called upon to prevent and respond to terrorist attacks.

Mr. Chairman, ODP has established an outstanding track record of capacity building at the State, local, territorial, and tribal levels, through strong and long-standing ties to the Nation's homeland security community. ODP has worked with Federal agencies and State and local jurisdictions to develop and disseminate information to assist in making more informed preparedness decisions, including capability assessments, preparedness planning and strategies, and choices relating to training, technical assistance, equipment, and exercises.

Since its creation in 1998, ODP has provided assistance to all 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and the U.S. territories. Through its programs and initiatives, ODP has trained over 575,000 emergency responders from more than 5,000 jurisdictions and conducted nearly 500 exercises. Since its creation, Homeland Security has provided states and localities with over $8.2 billion in State Homeland Security Grants for the purchase of specialized equipment to enhance the capability of state and local agencies to prevent and respond to incidents of terrorism involving the use of chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons; for the protection of critical infrastructure and prevention of terrorist incidents; for the development, conduct and evaluation of state CBRNE exercises and training

programs; and for costs associated with updating and implementing each states' Homeland Security Strategy. Since 2002, ODP has specifically provided $1.2 billion in grant assistance to States and local jurisdictions to improve interoperability through the purchase of communications equipment.

During Fiscal Year 2004, ODP's record of service to the Nation's first responders continues. All of the 56 States and territories have been awarded their Fiscal Year 2004 funding under the Homeland Security Grant Program. This includes funds to support State-wide preparedness efforts under the State Homeland Security Grant Program (SHSGP), the Law Enforcement Terrorism Prevention Program, and the Citizen Corps Program. These awards represent over $2.2 Billion in direct assistance.

Further, 50 urban areas designated under the Fiscal Year 2004 Urban Areas Security Initiative (UASI) have been awarded funding. This represents $671 Million in support to high-density population centers with identifiable threats and critical infrastructure. In addition, the Department has identified 30 of the Nation's most used urban transit systems and has provided $49.7 Million to enhance the overall security of these systems.

ODP's two primary sources of assistance to States and local communities, SHSGP and UASI, require States and Urban Areas to assess their risk, capabilities, and need, including requirements relating to interoperable

communications. These assessments and strategies have given us valuable information on the current State of interoperable communications and how various States and localities are addressing this issue. This is in fact the framework that we have been using to provide the technical assistance and training in the area of interoperable communications, which I will address in more detail later in my testimony.

As you will recall Mr. Chairman, on December 17, 2003, the President issued "Homeland Security Presidential Directive (HSPD)-8." Through HSPD-8, the President tasked Secretary Ridge, in coordination with other Federal departments, as well as State and local jurisdictions, to develop a national preparedness goal to improve the delivery of federal preparedness assistance to State and local jurisdictions, and strengthen the preparedness capabilities of Federal, State, territorial, tribal, and local governments.

Earlier this year, the Secretary delegated to ODP the responsibility for the implementation of HSPD-8. This designation by the Secretary is consistent with ODP's mission, as provided under Section 430 of Homeland Security Act of 2002, to be the primary Federal agency responsible for the preparedness of the United States for acts of terrorism. And ODP, together with Secretary Ridge, other Department components, Federal agencies, and State and local governments, firmly believe that the successful implementation of HSPD-8 is essential and critical to our Nation's ability to prevent, respond to, and recover

from acts of terrorism.

Through the work that is being conducted under HSPD-8, the Department will develop a national preparedness goal that will establish measurable readiness priorities and targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them. This effort will also produce readiness metrics and elements that support the national preparedness goal, including standards for preparedness assessments and strategies, and a system for assessing the Nation's overall preparedness to respond to major events. Among the principle issues to be addressed by these efforts will be interoperable communications.

In our efforts to meet the President's call to improve delivery of Federal preparedness assistance to State and local jurisdictions, ODP has made it a priority to not only provide assistance with preparedness assessments and grant funds to purchase new tools and equipment, but that needed training and technical assistance follows to insure full utilization of assets.

INTEROPERABLE COMMUNICATIONS TECHNICAL ASSISTANCE PROGRAM (ICTAP)

One of our most important technical assistance efforts to date is the Interoperable Communications Technical Assistance Program (ICTAP) which is

providing State, local, and tribal agencies with the operational support they need to get new interoperability systems up and running.

Section 430 (c)(2) of the Homeland Security Act of 2002 granted authority to ODP to serve as the primary agency responsible for "... coordinating, or as appropriate, consolidating communications and systems of communications relating to homeland security at all levels of government...". Under this mandate, ICTAP was initiated in August 2003 as part of Secretary Ridge's "One Stop Shop" to provide streamlined support for State and local preparedness programs. The program is designed to meet the legislative mandate of a direct link with States and urban areas for all homeland security related equipment acquisition, training, and technical assistance in the area of interoperable communications.

ICTAP provides technical assistance at no cost to jurisdictions in conjunction with the implementation of the State and UASI preparedness strategies. This program ensures that the jurisdictions understand the scope of their interoperability needs and how to fully utilize new technology.

The goal of the ICTAP program is to enable public safety agencies to communicate as they prevent or respond to a terrorism attack. ICTAP also leverages and works with other Federal, State, and local interoperability efforts whenever possible to enhance the overall capacity for agencies and individuals to communicate with one another. The ICTAP program is not limited to a set

time period, but focuses on quickly and thoroughly meeting the unique interoperability needs and requirements of jurisdictions across the country. However, it is also important to note that there are no "silver-bullet solutions" that we can drop-off in a region that will resolve its problems. From start to finish, interoperability requires a great deal of work with the key communication stakeholders in that region.

ICTAP – FOUR PHASED APPROACH

The ICTAP technical assistance team works closely with the Urban Area Working Group (UAWG), or its communication designees in the region, to provide on-site operational support from an initial assessment and inventory of what currently exists to live operation of the new system. The process covers four important phases:

Define Requirements: The ICTAP team can help the urban area assess its current communications capabilities and the interoperability gaps that limit communications between agencies at the local, State, Federal and tribal levels. This includes a survey of existing communications technologies and the development of operationally based scenarios to understand how agencies could respond to a terrorist incident and the interoperable communications capability needed to support that response.

Identify Solutions: The ICTAP team assesses a variety of potential solutions that could address the identified needs. Solutions may be short- and/or long-term, integrating other local, State, and Federal initiatives. Working with the input of the UAWG, the ICTAP technical assistance team develops an implementation plan.

Implement Solutions: The ICTAP team helps to implement and integrate the planned approach to interoperable communications, assisting with design of the chosen interoperable communications architecture and with implementation planning. This may include coordinating host site agreements, providing training, and assisting with testing.

Transition Services: The ICTAP team continues to provide technical assistance by assisting with training needs, utilization evaluations, and exercise coordination after the system is up and running.

The ICTAP approach is to provide long-term support which recognizes that each community has unique interoperability issues which require varying solutions. ICTAP's goal is to quickly and efficiently provide interoperability in the communities where we work, but we want to make sure it continues after we leave. ICTAP support will play a valuable role in implementing the HSPD-8 capabilities-based planning approach. HSPD-8 planning emphasizes a regional (mutual aid or assistance compact) approach to identification of required

capabilities, and the provision of expertise to State and local government planning bodies to aid in requirements identification and prioritization.

Program Facts and Figures

ICTAP has received requests for assistance from 32 of the 51 participating urban areas, as well as 8 States and 3 U.S. Territories. To date, the ICTAP program has been allocated $12.9 million. The current listing of the States, Regions and Territories in which we are working is noted on the next page.

Active UASI/ICTAP Sites	Pending UASI/ICTAP Sites	Active ICTAP Sites
Atlanta, GA	Buffalo, NY	Arizona
Baton Rouge, LA	Cincinnati, OH	Hawaii
Charlotte, NC	Columbus, OH	Idaho
Chicago, IL	Dallas, TX	Kentucky
Denver, CO	Detroit, MI	Louisiana
Fresno, CA	Las Vegas, NV	Missouri
Honolulu, HI	Minneapolis, MN	New Jersey
Houston, TX	Newark, NJ	Washington
Jersey City, NJ	Phoenix, AZ	
Kansas City, MO	Santa Ana, CA	**U.S. Territories ICTAP Sites**
Los Angeles, CA		
Miami, FL		
New Orleans, LA		Puerto Rico
New York City, NY		American Samoa
Oakland, CA		Virgin Islands
Orlando, FL		
San Diego, CA		
San Francisco, CA		
San Jose, CA		
Seattle, WA		
St. Louis, MO		
Tampa, FL		

ICTAP PUBLIC SAFETY EXPERTS & ENGINEERS

The ICTAP Program employs approximately 30 former public safety communications experts and technical engineers who have firsthand operational experience with emergency responder interoperability communications services and issues. ICTAP is using some of the best engineers and public safety practitioners in the nation. Our experts include former State and local communications administrators, members and former officers of the Association of Public Safety Communications Officials (APCO), former Statewide interoperability project managers and local public safety directors. To enhance coordination of Federal interoperability efforts, ICTAP also employs the National Consortium for Justice Information and Statistics, which is also providing training and technical assistance to the Department of Justice's COPS interoperability grantees. ICTAP technical support is provided by an experienced group of engineers from the Space and Naval Warfare Systems Center, San Diego (SSC-SD) who have successfully implemented interoperability solutions with the military and with State and local jurisdictions. SSC-SD has also been assigned by ICTAP to support the technical needs of the DHS RAPIDCOM 9/30 program.

SPECIFIC SITE INFORMATION

Within each State or region, ICTAP works to establish a steering committee, as well as a technical working group made up of the State, local, and tribal stakeholders who are directly responsible for communications. This work with

dozens of local jurisdictions has clearly demonstrated once again that there is no silver bullet for interoperability. I will discuss below in general terms some examples of ICTAP's work.

In addition, ODP conducted a trends analysis of common issues in communications interoperability resulting from the Fiscal Year 2003 State Homeland Security Assessment and Strategy (SHSAS) process and ODP exercise after action reports.

An analysis of the 56 strategies submitted through the SHSAS process reveals that a total of 54 States and territories address at least one of seven interoperable communications issues in their strategies. These issues are: plans, committees or working groups, assessments, equipment, training, exercises, and general statements regarding interoperable communications.

The results of the exercise trends analysis revealed several observations regarding gaps in communications interoperability, including: a high rate of non-interoperable radio frequency and radio channel usage; the fact that radio communications often are a patchwork of systems rather than an integrated approach to communications interoperability; and that protocols for mutual aid communications rarely exist.

Florida Sites

As an example, South Florida is devoting significant attention to the difficult policy issues of developing standard operating procedures and mutual aid agreements to address incompatible systems in that region's largest jurisdictions. At the same time, in Central Florida, the immediate issue is to document what equipment is in place throughout the region. In both areas, personnel are fully dedicated to communications issues in their own jurisdictions, making it difficult to dedicate the time necessary to complete these vital regional tasks.

To address these needs, ICTAP personnel have conducted face to face interviews with communications personnel in over a dozen jurisdictions in the Miami and Tampa areas to create regional inventories that will help these Urban Areas direct future funding requests for interoperable communications equipment, as well as determine what standard operating procedures (SOPs) and memoranda of understanding (MOUs) are needed. Personnel also were invited to support both the Free Trade Agreement of the Americas (FTAA) meeting in Miami, as well as the annual Gasparilla celebration in Tampa, to see communications systems in operation and prepare an "after-action-report" that was used by the local communication officials.

In the coming weeks, ICTAP will facilitate meetings with each Urban Area to make recommendations on how it can best "fill the gaps" in its communications strategy when Fiscal Year 2005 funding becomes available.

Kansas City Experience

Kansas City, Missouri, a UASI site that began to implement its ICTAP program in early 2004, provides an example of how the program is working with an ongoing interoperability effort. The Mid-America Regional Council (MARC), which has been designated by the State and the participating Urban Area as the Kansas City Urban Area Working Group, is a joint political organization of city and county governments that has been delegated the authority by these jurisdictions and the State to administer funds for the Kansas City metro area UASI program. "The ICTAP program has been a huge resource to the region," says Matt May, Emergency Services Planner for MARC. "In addition to funding, the ICTAP team has provided technical expertise that would have either severely decimated or eliminated funds allocated to the project, requiring MARC to look to other funding sources to initially implement the project" [Source: "Implementing the Interoperable Communications Technical Assistance Program (ICTAP)", U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, 2004.].

The proposed interoperability solution, known as the Regional Area Multi-Band Integrated System (RAMBIS) is a multi-band region-wide radio system that will provide interoperability between disparate radio systems (800MHz, VHF, UHF) through simulcast transmission and cross-band repeating. Simulcast transmission allows the same signal to be broadcast from multiple repeater sites to cover a larger geographic area. Cross-band repeat functionality will allow the channels for 800MHz, VHF, and UHF to be interconnected so that a transmission

received on one band will be rebroadcast on all bands, creating interoperability among all three frequency bands. With the Technical Working Group that ICTAP helped establish, efforts are underway to identify frequencies and facilities available for use by the RAMBIS system. In addition to contributing to the development of the Request for Proposal (RFP) for the RAMBIS system, the ICTAP team will assist with evaluation of RFP responses, and will be available to provide technical assistance during system implementation.

State of Idaho

Working with the Idaho Statewide Interoperability Executive Council (SIEC), the ICTAP program has provided technical support for the 700MHz feasibility study. ICTAP personnel have participated in five WMD exercises to collect interoperable communications data. Recognizing the need for documenting information about the current infrastructure throughout the State, ICTAP designed a web-based technical communications questionnaire and data collection tool which is currently being used to collect information. Over the coming months, ICTAP will support a comprehensive study of coverage and compatibility which will require eighty (80) site surveys, assessment of physical condition of existing radio frequency sites, inventory of existing equipment and documentation of tower structures. This support has been enthusiastically welcomed by the SIEC and the Governor's Office.

DHS COORDINATION

As we are all aware, there are a number of different activities both within DHS, as well as in other departments that involve interoperable communications issues.

The range of activities includes research, development and testing of interoperability solutions; defining industry standards; conducting nationwide baseline surveys; designing long term national interoperability strategies; and operational delivery of systems and training and technical assistance. These efforts are closely coordinated. The role of ICTAP is to fulfill the operational communications needs of States and regions.

All requests for ICTAP assistance are coordinated through the States to ensure consistency with State, and, where applicable, Urban Area homeland security strategies. This process streamlines the relationship between the requests for interoperability funding and the need for technical assistance and training to ensure it is used effectively. In the context of ICTAP's work, it is essential that we neither duplicate nor contradict any other Federal, State or local interoperability initiatives. In conjunction with our Federal partners, we have striven to present a coordinated approach. Examples of this coordination include:

Federal Inter Agency Board for Equipment Standardization and Interoperability (IAB)

ICTAP actively participates in the IAB and is a member of IAB sub-committee for Interoperable Communications and Information Systems (ICIS). Through the IAB, the ODP ICTAP has access to a wide range of technical and subject matter communications interoperability expertise. ICTAP has successfully engaged IAB/ICIS members and enlisted their support as a technical assistance resource

for ICTAP and to help implement interoperable communications solutions. The IAB has been instrumental in documenting communications interoperability roles and relationships at the State and local level throughout the full cycle of a critical incident, and has been a strong advocate for strengthening State and local response operations through better communications.

SAFECOM

While we have focused on local support, ICTAP is well aware of the importance of developing National interoperability policy. For guidance on these issues, ICTAP relies on SAFECOM, which is the Federal government's umbrella office for coordination of public safety interoperability programs, to provide standards and conduct research which can help our jurisdictions develop a better interoperable communications program. As an example, in ODP's Fiscal Year 2004 guidance for the Homeland Security Grant Program and UASI, we adopted the SAFECOM developed "Guidelines for Interoperability" as recommendations for use of funds. In addition, ICTAP is examining how to incorporate the findings from the recently developed SAFECOM Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability. The SoR contains interoperability scenarios describing how SAFECOM envisions technology enhancing public safety. In addition, ODP/SLGCP has entered into a Memorandum of Agreement (MOA) with SAFECOM to codify the areas in which we can work more effectively together. This includes continuation of ODP support for SAFECOM projects like RapidCom, as well as coordinating other

areas of mutual interest such as the dissemination of grant guidance and providing technical assistance in the field.

Federal Interagency Coordination Council (FICC)

ODP, as well as other Federal agencies, is a member of the Federal Interagency Coordination Council (FICC). The FICC, which is chaired by SAFECOM, seeks to avoid duplication, promote best practices and coordinate Federal grants and technical assistance among the Federal agencies supporting public safety interoperable wireless communications improvements.

RAPIDCOM 9/30

The contacts and relationships developed through ICTAP's work with first responders have also proven to be a valuable resource in furthering the initiatives of our fellow agencies. For example, when SAFECOM was tasked with RAPIDCOM 9/30 -- a major initiative announced by Secretary Ridge with the task of ensuring interoperability in America's ten largest cities by September 30, 2004 -- it was the SLGCP developed Urban Area Working Groups that were used as the primary points-of-contact for this effort. Furthermore, ICTAP personnel have participated in meetings with almost all of the RAPDICOM cities, and when asked, we also provided operational expertise in support of this initiative.

In Miami, Florida, for instance, the ICTAP program had been working with local communications personnel for a number of months when RAPIDCOM 9/30

began. SAFECOM staff was able to take advantage of existing ICTAP relationships and technical information to better focus their efforts. Furthermore, by closely coordinating this work, ICTAP will be able to utilize the work completed by SAFECOM long after September 30th as we continue our training and technical assistance to support Miami's interoperability efforts.

Department of Justice Coordination

Finally, by communicating with the Department of Justice about previous interoperability initiatives, ICTAP personnel have ensured that response agencies have incorporated this work into their homeland security interoperability efforts. For example, ICTAP has worked closely with personnel from the Department of Justice's Integrated Wireless Network and 25 Cities Program to ensure that the work completed to date on that project was properly coordinated and not duplicated by SLGCP.

CONCLUSION

In closing, DHS's mission is critical, its responsibilities are great, and its programs and activities impact communities across the Nation. We will strive to fulfill our mission and meet our responsibilities in an effective and efficient manner. And we will, to the best of our abilities, continue to identify where and how we can improve. Part of our responsibility, part of the Department's responsibility, Mr. Chairman, is the recognition that we can always improve what we do and how we do it. Mr. Chairman, let me restate Secretary Ridge's

commitment to support the Nation's State and local homeland security community, and to ensure that America's emergency responders receive the resources and support they require to do their jobs. This concludes my statement. I am happy to respond to any questions that you and the members of the Committee may have. Thank you.

Mr. PUTNAM. Thank you very much, and before we take our final testimony, I would like to welcome to the subcommittee our newest member, Ms. McCollum, the gentlelady from Minnesota. We will move forward with our testimony.

Our final witness on panel one is John Muleta. Mr. Muleta serves as Chief of the Wireless Telecommunications Bureau within the Federal Communications Commission. Prior to his appointment as Chief, Mr. Muleta served the FCC in various positions, including Deputy Bureau Chief in the Common Carrier Bureau and Chief of the Enforcement Division of that same bureau. In the private sector, he began his career at GTE Corp. and later worked at Coopers and Lybrand Consulting. He received a B.S. degree in systems engineering at the University of Virginia School of Engineering and Applied Sciences, and his J.D. MBA also from the University of Virginia. Welcome to the subcommittee, sir. You are recognized for 5 minutes.

STATEMENT OF JOHN MULETA, ESQ., CHIEF, WIRELESS TELECOMMUNICATIONS BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Mr. MULETA. Good afternoon, Chairman Putnam and other members of the subcommittee.

I'd like to note that I'm sitting beside my colleague from the Department of Homeland Security, one of the few times University of Virginia has been behind Virginia Tech. That's a little aside there. [Laughter.]

I want to thank you for this opportunity to appear before you on behalf of FCC to discuss our work on facilitating interoperability between the Nation's public safety communications systems. On July 20th of this year, I appeared before the committee to discuss our work on facilitating interoperability. On that date, GAO had released its comprehensive analysis on Project SAFECOM and testified as to the challenges that are inherent in fostering interoperability on a nationwide scale. During the past month, the Commission has taken several steps to further its efforts in this area. First, the Commission released its decision regarding public safety interference on the 800 megahertz band, which will go t a significant way toward alleviating and ultimately eliminating instances of interference to public safety in that band, while simultaneously freeing up additional spectrum for public safety use, including for interoperability purposes.

Second, the FCC's Homeland Security Policy Council report to the Commission on the FCC's overall efforts to ensure that our regulations and policies promote public safety interoperability, enhance 911 implementation, network security and reliability and other vital homeland security goals. In addition to our initiative, the 9/11 Commission released its report with its recommendations that may impact telecommunications policies.

Before discussing these important matters, however, I'd like to review the FCC's background and history in dealing with interoperability and public safety spectrum issues. The Commission's experience working with public safety entities and stakeholders is expansive and far-reaching. Today there are more than 40,000 spectrum licenses designated for public safety systems under the Commu-

nications Act. The FCC has the unique role of providing the spectrum that States and local governments use as an integral part of these systems.

Under the leadership of Chairman Powell, the Commission has intensified its effort in this area and designated homeland security and public safety issues as one of the Commission's six core strategic objectives. As September 11th vividly demonstrated, the ability of public safety systems to communicate seamlessly at incident sites with minimal onsite coordination is critical to saving lives and property. The FCC is therefore committed to using all of its resources to promote and enhance interoperability of the thousands of other safety systems that make up a critical part of our homeland security network.

Our experience indicates that a holistic approach is the best method for fostering interoperability. Achieving interoperability requires a focus on more than spectrum, technology and equipment issues. It also requires a focus on the organizational and the personal coordination communications that are necessary to make it available at the times of our greatest needs. For its part, the Commission directed its efforts toward providing additional spectrum for public safety systems, to also nurture technological developments that enhance interoperability and also providing its expertise and input within the limits of the statute to interagency effort such as SAFECOM to improve our homeland security.

With that said, it's important to understand that despite all its efforts, there are limits to what the FCC can do. The FCC is only one stakeholder in the process, and many of the challenges facing interoperability are a result of the disparate governmental interests, local, State and Federal, that individually operate portions of our national public safety systems. Each of these interests has different capabilities in terms of funding and technological sophistication, making it difficult to develop and deploy interoperability strategies uniformly throughout the country without initiatives such as the ones that SAFECOM and DHS are now implementing.

Regardless of these problems, we at the FCC continue to advance policies that enable all of the stakeholders to do their best in maintaining a strong and viable national public safety system.

Moving on to the actual spectrum that's available for public safety, the Commission currently has designated throughout the country approximately 97 megahertz of spectrum from 10 different bands for public safety use. The Commission has also designated channels of these public safety bands specifically for interoperability, including 2.6 megahertz in the 700 megahertz band, five channels in the 800 megahertz band, five channels in the 150 megahertz band which is commonly known as the VHF band, and four channels in the 450 megahertz band, known as the UHF band.

In addition, starting next January, the Commission will require newly certified public safety mobile radio units to have the capacity to transmit and receive on a nationwide public safety interoperability calling channel in the UHF and VHF bands in which they operate.

In recent years, the Commission has also made additional spectrum available for public safety use. First, consistent with the Balanced Budget Act of 1997, the FCC identified and allocated 24 ad-

ditional megahertz of spectrum in the 700 megahertz band for public safety use. In particular, it's important to note that the FCC designated 2.6 megahertz of the spectrum for interoperability purposes. Given the central role the States provide in managing emergency communications and in concert with what my colleague from GAO has reported on, the FCC also concluded that States are well suited for administering the interoperability spectrum and that State level administration would promote the safety of life and property through seamless coordinated communications on interoperable spectrum.

Second, the FCC designated 50 megahertz of spectrum at 4.9 gigahertz for public safety users in response to requests from the public safety community for additional spectrum for broadband data communications. The 4.9 gigahertz band rules also foster interoperability by providing a new and innovative regulatory framework where traditional public safety entities can pursue strategic partnerships with others, such as a critical infrastructure industry, that are necessary for the completion of their mission.

Most recently, in our July agenda meeting, the Commission adopted by unanimous and bipartisan vote a solution to the ongoing and growing problem of interference based in the 800 megahertz public safety radio system. In addition to providing a means to abate such interference, the Commission's decision will ultimately result in the availability of additional 4.5 megahertz of the 800 megahertz band, which is the most heavily used band for public safety and critical infrastructure licenses. We are hopeful that public safety organizations will take full advantage of this additional spectrum to advance interoperable communications goals.

Moving on to the coordination efforts that we carry on, the Commission staff also routinely confers and does outreach with critical organizations, including the Association of Public Safety Communications Officials, the National Public Safety Telecommunications Council, the International Association of Fire Chiefs, International Association of Chiefs of Police. Moreover, the staff is working closely with the Department of Homeland Security SAFECOM as we both share the common goal of improving public safety communications and interoperability. We are continuing our collaborative efforts to develop a strong working relationship, both formally and informally.

Dr. Boyd and I also continue to work together at a personal level to promote and ensure effective coordination regarding homeland security issues. As I mentioned in July, Dr. Boyd and I are committed to establishing an informal working group comprised of representatives of our respective staffs to meet on a regular basis to focus on interoperability issues of mutual interests. I am pleased to announce that we have taken steps to this end, and just recently, representatives of our staff have initiated this effort. I am encouraged by this action and confident that this interagency cooperation will prove beneficial to all the groups involved.

Thank you for the opportunity to testify in front of you on this important issue, and I will be glad to answer any questions you might have. Thank you, sir.

[The prepared statement of Mr. Muleta follows:]

WRITTEN STATEMENT

Of

JOHN B. MULETA, Esq.
Chief, Wireless Telecommunications Bureau
Federal Communications Commission

Hearing

On

Project SAFECOM: More Time. More Money. More Communication?
What Progress Have We Made In Achieving Interoperable Communication Between Local, State, and Federal First Responders?

Before the
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
House Government Reform Committee

September 8, 2004
2:00 p.m.
2154 Rayburn House Office Building
Washington, D.C.

Written Statement of John Muleta, Esq.
Chief, Wireless Telecommunications Bureau
Federal Communications Commission

Introduction

Good morning Chairman Putnam, Ranking Member Clay and Members of the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. Thank you for this invitation to appear before your subcommittee on behalf of the Federal Communications Commission (Commission or FCC) to provide an update on our continued progress in promoting interoperability among our nation's first responders.

On July 20, 2004, I appeared before the Government Reform Committee's Subcommittee on National Security, Emerging Threats and International Relations to discuss our work in facilitating interoperability. On that day, the Government Accountability Office released its comprehensive analysis of Project SAFECOM, and testified as to the challenges inherent in fostering interoperability on a nationwide scale. During the past month, the Commission has taken several steps to further its efforts in this area. First, the Commission released its decision regarding public safety interference in the 800 MHz band, which will go a long way toward alleviating and ultimately eliminating instances of interference to public safety in that band, while simultaneously freeing up additional spectrum for public safety use. Second, the FCC's Homeland Security Policy Council (HSPC) reported to the Commission on the FCC's overall efforts to ensure that our regulations and policies promote public safety interoperability, Enhanced 911 (E911) implementation, network security and reliability, and other vital Homeland Security goals. Also, since I last testified, the 911 Commission released its report, which contains some recommendations that could have an impact on telecommunications policies.

Before discussing these important matters, I would like to review the FCC's background and history in dealing with interoperability and public safety spectrum issues. As you are aware, the Commission's experience working with public safety entities and stakeholders is expansive and far-reaching. Congress began working in this area shortly after the Titanic disaster and today there are more than 40,000 station licenses designated for public safety systems under the Communications Act. The FCC has the unique role of providing spectrum for state and local governments to use as part of these systems. As a result, the Commission has a long-standing commitment to the protection and enhancement of public safety communications systems.

Under the leadership of Chairman Michael K. Powell, the Commission has intensified its efforts and designated homeland security and public safety issues as one of the Commission's six core strategic objectives. As September 11, 2001 demonstrated, the ability of public safety systems to communicate seamlessly at incident sites with minimal on-site coordination is critical to saving lives and property. The FCC remains committed to using all of its resources to promote and enhance the interoperability of the thousands of public safety systems that make up a critical part of our nation's homeland security network.

The Commission's experience indicates that a holistic approach is the best method for fostering interoperability. Achieving interoperability requires an emphasis on more than spectrum, technology and equipment issues – it also requires a focus on the organizational and personal coordination and communication necessary to make interoperability available in times of greatest need. For its part, the Commission directs its efforts toward allocating additional spectrum for public safety systems, nurturing technological developments that enhance interoperability and providing its expertise and input for interagency efforts such as SAFECOM.

There are limitations, however, to what the FCC can do. The Commission is only one stakeholder in the process and many of the challenges facing interoperability are a result of the disparate governmental interests – local, state, and federal – that individually operate portions of our national public safety system. Each of these interests has different capabilities in terms of funding and technological sophistication, making it difficult to develop and deploy interoperability strategies uniformly throughout the country. Regardless of these challenges, we at the FCC continue to advance policies that enable all of the stakeholders to do their best in maintaining a strong and viable national public safety system.

Commission Resources

The FCC works in an integrated and flexible fashion to assign spectrum for public safety purposes. The Wireless Telecommunications Bureau (WTB) and the Office of Engineering and Technology (OET) share significant responsibility for intra-agency projects related to interoperability technology and policy development. The Commission also maintains the HSPC and created the Office of Homeland Security (OHS) within the Enforcement Bureau to facilitate intergovernmental communications on Homeland Security issues.

Wireless Telecommunications Bureau

WTB underwent reorganization this past year and created the Public Safety and Critical Infrastructure Division (PS&CID). PS&CID administers the licensing rules for public safety radio networks and the related radio networks of critical infrastructure industries such as the nation's utilities. The division also has the responsibility of promulgating rules that require wireless carriers to deploy E911 systems throughout the country for the benefit and use of over 160 million cell phone subscribers – another critical element of the nation's homeland security

system. The division's routine day-to-day contact with public safety licensees, their vendors and other stakeholders allows it to closely monitor industry trends and needs. In 2003, WTB processed more than 529,000 public safety and other private land mobile applications, including applications for new licenses, license modifications and renewals, waivers, and requests for special temporary authority.

Office of Engineering and Technology

In addition to its responsibility for spectrum allocations, OET routinely assesses vulnerabilities in communications networks and equipment and makes recommendations for facilitating improvements to network security, reliability and integrity. OET also evaluates new technologies and makes recommendations to the Commission for rule changes which would enable their use to improve the communications capability of the nation's public safety community. OET is the agency's principal point of contact with the National Telecommunications and Information Administration (NTIA) and in this role works with NTIA on spectrum issues that affect both non-Federal and Federal government spectrum users, including state, local and federal first responders.

Homeland Security Policy Council and Office of Homeland Security

The FCC's HSPC, created in November 2001 and composed of senior managers of the Agency's policy bureaus and offices, and the OHS assists the Commission in implementing the Homeland Security Action Plan. Among the directives of the Action Plan is to ensure that public safety, public health, and other emergency and defense personnel have effective communications services available to them as needed.

Homeland Security will continue to be a focal point of the Commission's work. We are very proud of our achievements to date and look forward to building upon these accomplishments to reach new heights in this very important area. Last month, at the FCC's Agenda Meeting, HSPC reported on the status of the Agency's progress with respect to its homeland security objectives. The Commission's staff reported that in the last year alone, the FCC has considered several key proceedings that should have a dramatic, real world impact on Homeland Security. These proceedings include the 800 MHz proceeding, the 4.9 GHz proceeding, and the Intelligent Transportation Systems proceeding. As many of you may know, earlier this summer, the Commission adopted a plan for the 800 MHz band to resolve the problem of interference to public safety radio systems. As mentioned previously, this plan also made additional available spectrum for public safety uses. In the 4.9 GHz proceeding, the Commission accommodated a variety of new applications that will permit, for example, the delivery of floor plans to policemen entering a hostile environment and real time video from inside a burning building. In the Intelligent Transportation Systems proceeding, the Commission advanced benefits such as the ability to monitor traffic from a control point and to direct first responders along the path of least resistance. The Commission considered proceedings that promote new technologies, such as radio frequency ID tags and cognitive radios.

Our proceedings reveal only part of the story. Our expansive outreach efforts have been equally important in achieving our Homeland Security goals. HSPC and OHS ensure coordination with other federal, state, and local entities that are involved with Homeland Security. For example, as a partner with the Department of Homeland Security, the FCC has promoted registration of states and localities in the Telecommunications Service Priority and the Wireless Priority Access Service programs. These programs provide wireline and wireless

telephone dial tone to public safety entities on a priority basis during and following a disaster. HSPC members also are working with disabilities rights organizations to identify and resolve communications issues that have an impact on that community during national emergencies.

In addition, HSPC and OHS work closely to support the Network Reliability and Interoperability Council (NRIC VII) and Media Security and Reliability Council (MSRC), two of the FCC's federal advisory committees. Through NRIC VII, communications industry leaders provide recommendations and best practices to the FCC focused on assuring optimal reliability and interoperability of wireless, wireline, satellite, paging, Internet and cable public communications networks and the rapid restoration of such services following a major disruption. MSRC does much the same with the goal of achieving optimal reliability, robustness and security of broadcast and multi-channel video programming distribution facilities. Public safety representatives are part of this effort since, during emergencies, TV and radio are sources of information for citizens.

Coordination

The FCC recognizes that interagency coordination is an essential factor in developing effective interoperability. To that end, Commission staff routinely confers with the Department of Homeland Security's SAFECOM. The FCC and SAFECOM share the common goal of improving public safety communications interoperability. We are continuing our collaborative efforts to develop a strong working relationship, both formally and informally. For example, the FCC is an active member of SAFECOM's Advisory Group. In addition, FCC staff has met with staff from SAFECOM on several occasions for information exchanges and briefings, including, most recently, a March 11, 2004 presentation to SAFECOM's Executive Committee on matters pending before the Commission. FCC staff also has attended and participated in several events

hosted by SAFECOM, including its 2003 Summit on Interoperable Communications for Public Safety and 2004 Public Safety Communications Interoperability Conference.

DHS Deputy Director David Boyd and I continue to work together to further promote and ensure effective coordination regarding homeland security and public safety communications initiatives. We agree that it is critical that the FCC and SAFECOM work cooperatively to achieve our common interests of promoting homeland security and interoperability. With this goal in mind, we have made a commitment to establish a working group comprised of representatives of our respective staffs who will meet on a regular basis to work collaboratively on interoperability and other issues of relevance to the FCC and SAFECOM. We envision that this new inter-agency "team" will provide an effective forum for informed, innovative and on-going exchanges aimed at ensuring steady progress towards achievement of nationwide interoperability capability. I anticipate that the informational exchanges among the new inter-agency "team" would be in addition to our continued efforts at the executive level. We look forward to participating in SAFECOM's Executive Committee meeting scheduled for later this month in Washington, D.C., as well as other future opportunities in this regard.

Spectrum Designated for Public Safety Interoperability

The Commission currently has designated throughout the country approximately 97 MHz of spectrum from ten different bands for public safety use. Public safety entities also actively use other bands for a variety of services, including such new ultra-wideband equipment authorized by our rules which can be used for ground penetrating radars and imaging systems that enable public safety officers to detect the location or movement of people behind or within walls or other structures, an important and potentially lifesaving tool. In addition, the Commission has designated certain channels in the public safety bands specifically for

interoperability. A public safety entity may use these designated frequencies only if it uses equipment that permits inter-system interoperability. The frequencies that have these so-called "use designations" include 2.6 MHz of the 700 MHz band, 5 channels in the 800 MHz band, 5 channels in the 150 MHz band (VHF Band), and 4 channels in the 450 MHz band (UHF Band).

Starting on January 1, 2005, the Commission will require newly certified public safety mobile radio units to have the capacity to transmit and receive on the nationwide public safety interoperability calling channel in the UHF and VHF bands in which it is operating. Also, in the case of certain inland areas, known as VHF Public Coast areas (VPCs), the Commission has designated several additional channels in the VHF band to be used exclusively for interoperable communications.

Recent Public Safety Spectrum Allocations

The Commission is committed to ensuring that public safety operators have sufficient spectrum that is free from harmful interference. In addition to the recent release of the 800 MHz Order, the Commission has made two other allocations, in the last few years, that illustrate the importance placed on ensuring that public safety entities have sufficient spectrum to carry out their critical missions. First, consistent with the Balanced Budget Act of 1997, the Commission identified and allocated 24 MHz of spectrum in the 700 MHz band for public safety use. Second, the Commission made available for public safety use, 50 MHz of spectrum at 4.9 GHz.

<u>800 MHz</u>

On July 8, 2004, the Commission adopted – by a unanimous, bipartisan vote – a solution to the ongoing and growing problem of interference faced by 800 MHz public safety radio systems. In addition to providing a means to abate such interference, the Commission's decision will result in an additional 4.5 MHz of 800 MHz-band spectrum becoming available for public

safety and critical infrastructure licensees. The plan devised in the 800 MHz proceeding will have a direct impact on our first responders and will immediately benefit them, by ensuring that firefighters and policemen hear each other, not static, when keying up their radios. This proceeding was one of the most challenging in our Agency's history and presented a unique opportunity to promote and lend support to public safety communications operators.

The plan adopts a two-prong solution to interference abatement. To address the problem in the near term the Commission established an objective standard for defining "unacceptable interference" to public safety and other 800 MHz non-cellular systems. Any entity causing unacceptable interference must immediately cure it at its own expense, using a variety of technical solutions called "Enhanced Best Practices."

As a long-term solution for abating unacceptable interference, the Commission ordered reconfiguration of the 800 MHz band. In general, the Commission is segregating fundamentally incompatible technologies as far apart as possible in the 800 MHz spectrum. Public safety and other so-called "high site" systems have been grouped in the lower portion of the band; and the "low-site" cellular architecture systems -- the source of most of the interference -- occupy the upper portion of the band. This complex, nationwide reconfiguration of the 800 MHz band must be completed within thirty-six months. As I mentioned, at the conclusion of band reconfiguration, public safety and critical infrastructure licensees will have an average of 4.5 MHz of new spectrum available. We are hopeful that public safety organizations will take full advantage of this additional spectrum to advance their interoperable communications goals.

700 MHz

To better facilitate use of the 700 MHz public safety spectrum, the Commission adopted mandatory interoperability. Every voice and narrowband data radio used in the 700 MHz band must be able to access specifically designated interoperability channels, using a common communications protocol, thus providing "instant interoperability" for every new entrant into the band. The 700 MHz band also contains channels dedicated to wideband data signals, such as real-time video, transmission of fingerprints, mug shots, blueprints and other graphical material that first responders may need in the field. Given the central role that states provide in managing emergency communications, the Commission concluded that states are well-suited for administering the 700 MHz interoperability spectrum and determined that state-level administration of the interoperability channels would best promote safety of life and property through seamless, coordinated communications on the interoperability spectrum.

The FCC's rules provide that the states may manage interoperability channels in two ways. First, they may establish a State Interoperability Executive Committee (SIEC) or its equivalent; or, second failing that, the Commission- established Regional Planning Committees (RPCs) gives oversight of the 700 MHz spectrum. Thirty-eight states and the District of Columbia have elected to administer their interoperability spectrum. For the fourteen who did not, the RPCs have been delegated that responsibility.

From the beginning, the Commission has recognized that the utility of this spectrum for public safety depended on taking actions, consistent with the current statutory scheme, to minimize, and ultimately clear, the broadcast use of this spectrum. For instance, during the digital television (DTV) transition planning, the Commission minimized the use of channels 60-69. As a result, the new 700 MHz public safety spectrum on TV channels 63-64 and 68-69 is available now in many areas of the country. Because of the significance of this spectrum for

public safety, especially first responders, and interoperability, the Commission is actively considering ways to bring the digital transition to its conclusion. Indeed, under the direction of Chairman Powell, the Media Bureau has developed a bold framework that would provide a soft landing and a clear conclusion for the DTV transition so that, in part, we can provide public safety with this additional spectrum. In executing its proposal, the Media Bureau's objectives include: 1) bringing the transition to a timely and predictable conclusion; 2) reclaiming valuable spectrum; 3) minimizing disruption to consumers; 4) maintaining consumer access to HDTV and other digital services; and 5) complying with Constitutional and statutory requirements. Under this plan, the public would reclaim a significant amount of spectrum by January 1, 2009. In addition to advances in homeland security, public interest benefits will include broadband deployment, economic growth and job creation. The Commission is cognizant of the emphasis placed on spectrum availability in the 700 MHz band, and is aware of the discussion contained in the 911 Commission Report.

4.9 GHz

The Commission's allocation of 50 MHz of spectrum at 4.9 GHz (4940-4990 MHz) promises to permit the use of new advanced wireless technologies by public safety users. This spectrum is part of a transfer of Federal Government spectrum to private sector use. The Commission initially proposed to allocate the 4.9 GHz band for fixed and non-aeronautical mobile services and to auction it to commercial users, with no designation of the spectrum for public safety use. In response to requests from the public safety community for additional spectrum for broadband data communication, the Commission designated the 4.9 GHz band for public safety use in February 2002 and adopted service rules in April 2003.

The 4.9 GHz band will accommodate a variety of new broadband applications such as high-speed digital technologies, broadband mobile operations, fixed "hotspot" use, wireless local area networks, and temporary fixed links. The 4.9 GHz band rules will also foster interoperability, by providing a regulatory framework in which traditional public safety entities can pursue strategic partnerships with others necessary for the completion of their mission.

Licenses for this spectrum will be granted to public safety entities based on a "jurisdictional" geographical licensing approach. Accordingly, the 4.9 GHz spectrum will be licensed for shared use. Under this approach, the Commission will authorize 4.9 GHz licensees to operate throughout those geographic areas over which they have jurisdiction and will require them to cooperate with all other 4.9 GHz licensees in use of the spectrum. In order to increase spectrum use and foster interoperability, the Commission will permit licensees to enter into sharing agreements or strategic partnerships with both traditional public safety entities, including Federal Government agencies, and non-public safety entities, such as utilities and commercial entities.

Promotion of Public Safety Interoperability

There are a range of mechanisms that specifically promote interoperability. As discussed above, the Commission has used its resources to identify additional spectrum. The Commission also has provided for innovative licensing methods, created planning methods that encourage better coordination, and promoted new technologies.

Regional Planning

The Commission adopted the regional planning approach to spectrum management as an alternative to the traditional first-in-the-door approach to spectrum licensing and management in

the public safety context. Regional planning allows for maximum flexibility of the RPCs to meet state and local needs and encourage innovative use of the spectrum to accommodate new and as yet unanticipated developments in technology and equipment. The Commission has utilized this approach for public safety spectrum in the 700 and 800 MHz bands.

Sharing of Radio (Spectrum) Facilities

In order to promote interoperability, the Commission has rules for two types of spectrum sharing. First, the FCC's rules specifically provide for shared use of radio stations where licensees, including federal government entities, may share their facilities on a nonprofit, cost shared basis with other public safety organizations as end users. In July 2000, the Commission expanded this sharing provision. This rule also allows Federal government entities to share these facilities as end users. A second type of sharing, unique to the 700 MHz public safety spectrum, permits state and local public safety licensees to construct and operate joint facilities with the Federal government. The Commission took this action to encourage partnering of FCC-licensed state or local government entities with Federal entities to promote interoperability and spectrum efficiency.

Public Safety National Coordination Committee

The Public Safety National Coordination Committee (NCC) operated as a federal advisory committee from 1999 to 2003 and recommended technical and operational standards to assure interoperability in the 700 MHz public safety band. The over 300 members employed a consensus-based decision-making process to meet its charge. The NCC was guided by an eleven-member Steering Committee and used three subcommittees, each of them having several

working groups to develop its recommendations, many of them highly technical. It submitted its final recommendations in July 2003.

The NCC developed recommendations on a technical standard for the narrowband voice and data channels to ensure that police, firefighters, EMS and other public safety officials using 700 MHz radios can communicate with one another instantly on common voice and data channels. The same channels are designated for interoperability use everywhere in the United States. The Commission adopted the narrowband voice and data standard in January 2001 as the NCC recommended.

The NCC also developed a recommendation for a wideband data standard and forwarded it to the Commission in July, 2003. This standard would give public safety agencies a common "pipeline," on 700 MHz wideband data interoperability channels, with which to implement such applications as sending mug shots and fingerprints to police vehicles, medical telemetry from EMS units to hospitals, blueprints of burning buildings to firefighters, and video coverage of incidents to the incident commander. The NCC worked with the Telecommunications Industries Association – an accredited standards developer – to develop interoperability technical standards that are open and non-proprietary. The Commission will consider the remaining NCC recommendations, including the wideband data standard, in a future rulemaking.

Intelligent Transportation Systems Radio Service

In December 2003, the Commission adopted service and licensing rules for the Dedicated Short Range Communications (DSRC) Service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850-5.925 GHz band. It is envisioned that DSRC would provide the critical communications link for ITS, which is key to reducing highway fatalities, a high priority for the Department of Transportation. The effective and expeditious implementation of DSRC

not only benefits American consumers by providing solutions to today's transportation challenges and allowing life-saving communications. It also provides public safety entities with another communications tool that can assist them in fulfilling their missions. To ensure interoperability and robust safety and public safety communications among DSRC devices nationwide, the Commission adopted rules requiring that the ASTM-DSRC standard be used. The Commission also adopted licensing and technical rules aimed at creating a framework that ensures priority for public safety communications, thereby allowing both public safety and non-public safety use of the 5.9 GHz band. Further, the Commission adopted a jurisdictional licensing approach similar to that used for the 4.9 GHz band.

Cognitive Radios Proceedings

The Commission is actively exploring the potential of new technologies to enhance interoperability and encourage network efficiency of public safety systems. One example of such new technologies is cognitive radios, which have the capability to change their power and/or frequency, sense their environment, know their location, and optimize their communication path. This technology holds tremendous promise for public safety interoperability by making it possible for radios from different public safety systems to operate seamlessly at an incident site without prior coordination. The Commission has initiated a proceeding to examine the enhanced interoperability potential that these even more flexible technologies may offer.

Conclusion

Public Safety Interoperability is a key component of an effective homeland security network, and the FCC is cognizant of the importance of facilitating related communications

systems. The FCC is dedicated to marshalling all of its resources and expertise in order to ensure that adequate spectrum and technology is available for providing interoperability among the nation's public safety systems. The Commission continues to work with a wide range of stakeholders to foster and promote new policies, rules, regulations and technologies related to public safety interoperability. Although some of the challenges involved in bringing interoperability to public safety systems are outside the scope of the FCC's authority, the Commission continues to take a leadership role in trying to resolve these challenges. Thank you for the opportunity to testify on these important issues affecting our homeland security.

Mr. PUTNAM. Thank you very much. I know that there will be a number of questions. We will begin with 5 minute rounds. The Vice Chair of the subcommittee will begin, the gentlelady from Michigan, Ms. Miller.

Ms. MILLER. Thank you, Mr. Chairman.

I appreciated all of you coming today and your testimony is very interesting. One of the more emotional debates I think that we had this year on the floor of the House was when we were debating the Department of Homeland Security budget. There was an amendment that just about everybody had something to say about, where they were talking about whether or not we should be expending more funds in the State of New York, in the city of New York rather than spending funds in Montana or Wyoming. This is not a new debate. I think the entire Nation has engaged in it. In fact, I noticed recently one of the networks had a story about this. I forget the numbers numerically, but I think they were saying that some of the less populated States were getting almost $50 per capita, States like New York, etc., were in the $20 range or something. Again, I've forgotten the numbers, but quite a discrepancy there.

So I have a question about the dollars as well, and how we actually are expending the dollars. I think Dr. Boyd and Mr. Beres both mentioned a little bit about the dollars. Whether or not, I think Mr. Boyd said there was quite a bit of money that we had never before authorized so much money for the DHS and for the various programs. I think Mr. Beres mentioned the $2 billion amount.

But I'm just wondering, first of all, how much actually has been authorized by Congress in regards to SAFECOM and how are you actually granting the dollars? Especially I guess my question goes to, how are you actually working with the States or localities? It's been my experience in Michigan that it's almost exclusively with the State of Michigan rather than the individual counties. I'm just wondering if that is true or my observation is correct, and are you then working with the States, each one of the States of course is responsible to have their respective department of homeland security assessment, their State assessment? How is all this working?

Mr. BOYD. I think we probably ought to answer that in two parts. Tim Beres manages the actual grant funding. Let me talk a bit about how we're approaching the States and what we think it requires to make things work in the States.

We're convinced that for any statewide plan to work, and we think you need a statewide plan, it has to be one that's built from the bottom up, that includes the small counties and the small towns. When we worked with the State of Virginia to help them develop a statewide plan, we intentionally started the effort in Wytheville, VA, a very small place, and then worked our way around the State. In fact, that statewide plan is attached to testimony that you will be hearing in the next panel.

We believe you can't make interoperability work unless you start at the local level and work your way up. Because interoperability isn't something that's isolated to a single city or a single place, if we're going to have real interoperability you have to be able to take it to all levels. For example, when urban search and rescue teams deploy, no matter where it is they go they come from a variety of jurisdictions. They don't just come from big cities; they often come

from volunteers in smaller counties, from a combination of groups from around the United States.

It's important when they arrive that their communications equipment be fully interoperable. The way it's handled now in many cases is exactly as the chairman has pointed out, by exchanging radios. They either bring extra radios with them, or the agency that they're coming to support has to provide them radios. We need to be able to do a much better job than that, and we think that means you have to start with a collaborative effort that includes all of the players at the very lowest level of government all the way up to the very highest level. It's our experience that no statewide plan will work unless it's built this way.

Ms. MILLER. Tim.

Mr. BERES. Thanks. The majority of our funding goes through the States, as you mentioned before, both the urban Area Security Initiative funding and the State Homeland Security grant program does go through the States. Then it has to be, 80 percent of those funds have to be sub-granted out to local units of government.

The reason for this is to allow the State, a central player, to have an overall look, strategic look, strategic planning outlook, as to how to allocate the funds. This is especially important when we're talking about interoperability, so that we aren't making individual grants to smaller communities that aren't necessarily incorporated into an overall broader plan or broader strategy for interoperability. We want to make sure that coordination is done at a central level in the State, along with all the communities that would be receiving funding for interoperability.

Ms. MILLER. You know, if I could followup on that, a big purposes of this hearing today is so that we can continue to fine tune and do a better job and make sure the dollars are getting where they need to get. It's not as though we all just fell off the truck and now find out that the ability to communicate is a problem. It's not as thought it's inherent to one particular area. It seems to be very widespread.

In fact, I'll give you a personal experience, Secretary Ridge came into one of my counties, and that's what he said, almost everywhere he went in the Nation, that's what he was finding, is the ability to communicate amongst the various first responders and public agencies, etc., was a big problem that we were having. I'm wondering whether or not Congress, for instance, maybe we have made the criteria for the granting too restrictive for you. I have a county in my area, all politics being local, this is the county that has the Bluewater Bridge, which is the third busiest commercial artery on the northern tier, it is the only bridge that is authorized to transport hazardous material. We have a CN Rail tunnel that's immediately under there. We have something called Chemical Valley that runs along, we have a liquid border that we share with Canada for miles and miles with all these chemical plants, etc.

And yet almost all the money that comes into our State seems to go into a county that is host to the city of Detroit, because of these population criteria that we have foisted on all of you. Is there a way that Congress can make you better able to accomplish your mission, give you more flexibility? Do you have any comments on

how restrictive we've made it in handicapping your ability to get the dollars?

Mr. BERES. There's two different programs that we have, one of which is the Urban Area Security Initiative program, which is based on risk primarily, a risk-based formula that really hits to the highest threat urban areas in the country, one of which is Detroit and its core county that is around it. Then the other program is a little bit larger than the Urban Area Security Initiative Program, which is a statewide program, which is, the purpose of that is to meet those other areas that are not covered under those high risk programs.

So we do focus a great deal of our dollars on high risk areas that have been identified, but then a whole other pot is focused on high risk areas that the State has identified that aren't in our original pot. Some of those can be pushed to those other areas through the State itself.

Mr. BOYD. We also had some other difficulties as we applied the common grant guidance. Depending on who it was they were applying to for the grant, and what legislation governed the agency, the rules for the grants were different. So with SAFECOM grant guidance we tried to create a common set of requirements, but then we had to tailor them based on what the law actually said, for whether it was a grant that was coming through FEMA or it was a grant coming through the COPS office or it was part of a State block grant coming through the State.

In some cases the grants would permit funding only for equipment. One of the great difficulties with this is that many of these localities lack the technical expertise, the engineering help, and the consulting help they needed. But in the case of the COPS grants, they could spend the money only on equipment. In the FEMA grants, they had a bit more flexibility and they were actually able to use these to pay for all the elements of interoperability.

One of the points we make, and one of the reasons we developed the continuum is that technology is only one component of interoperability. You also have to help the jurisdictions develop solid governance structures, you have to work with them through exercises and training, you have to help them develop standard operating procedures, and you have to be able to provide the technical assistance they need. So it would be useful if mechanisms were made available, if the legislation didn't have different requirements to address the same problem, and if they weren't so restrictive that communities couldn't seek the kind of help they needed in order to support interoperability.

Ms. MILLER. Thank you.

Mr. PUTNAM. Thank you, Ms. Miller.

I'd be happy to recognize the gentlelady from Minnesota for your first wave of questioning.

Ms. MCCOLLUM. Thank you, Mr. Chair.

I just had a meeting with the first responders' representatives in Minnesota with Congressman Szabo this past month in August. And there were a couple of themes that came up, and of course they all had to do with dollars. One of them was just in applying for the grants, and I noticed in the GAO study it talks about Federal grant structure does not support statewide planning. And an-

other section of it deals with grant submission, performance period, time, also presents challenges to short term and long term funding.

One of the issues, and everybody around the table shook their head, is the supplying online that they're doing. The system is down for maintenance quite often on the weekends. These are people who are putting this on top of already a 40 hour work week that they're doing, quite often coming in to do this on evenings and weekends. And the system is down for maintenance, they can't, I'll get you their comments. But they were really looking to having a system that was user friendly and easy to use. There is room for needs improvement in this category for our local elected officials.

The other issue was the way that reimbursements were being held. They have budgets and budget frames in which they work under for county and local units of government. The Federal budget frame doesn't work the same way. And they are not allowed to run deficits, they have to balance their budget. So they either have to make decisions that the grant is going to forward and the funding will come when they submit their budgets to, whether it's a city council or the county or the State. Then if it doesn't come, they've created a deficit, a hole in their budget.

So I hope as we move forward and along with this, we take into account not only do we need to get our work done for our budgeting in a timely fashion, that is stay here and do the work, but we also have to be cognizant of what their budgets are like. And also the joint powers agreement that many municipalities have to enter into in order to make their projects cost effective also is causing problems in applying for grants.

So having said that, I'll move to the two questions that I have. One is in a document that was prepared for us and it's on page three. It talks about the GAO, however, according to the Department of Homeland Security, failed to secure agreements with two of the key stakeholder agencies in 2003, the Departments of Interior and Justice. Thus, only $17 million of the $30.9 million OMB allocated through participating agencies was received by SAFECOM. So my question is, what happened to the other $18 million?

And I also have heard very clearly from my first responders, both private sector and public sector, that they are very concerned about interoperability continuing on in the future as technology upgrades will be happening. First they are trying to get the money to convert everybody to 800, then they have the challenge of how do we keep everybody from the National Guard to the smallest township in Ramsey County current with upgrades? Has there been any talk about how we're going to play for the money for that?

Mr. BOYD. Well, let me answer the first question about the partner funding. So far we have agreements in place and have received the funding this year from all of the partners except the Department of Interior. We continue to talk with the Department of Interior. But all the rest this year has been provided.

Part of the SAFECOM planning makes the assumption that we're going to have a variety of different technologies over time. That's because technology doesn't advance in an orderly way and localities can't simply upgrade every time something new arrives on the horizon.

So for that reason, we believe the development of our standard strategy and the kinds of help we provide to localities needs to provide what we call a migration path; that is, a rational way to migrate forward to full interoperability while maintaining backward interoperability with legacy systems. We know, for example, that software defined radio is on the horizon. We know that increasingly we're going to be moving from analog to digital systems. And so all of those are going to continue to create some of the technology disconnects that contribute to a lack of interoperability.

There are near term ways to get around this, and part of what RAPIDCom is focused on doing and what we're trying to help localities with is to put into place near term interoperability solutions, things like patch devices. We, for example, issued a set of specifications to govern the purchase of patch devices that localities could use when they issued their requests for proposals from manufacturers.

We think all of those things, together with a standards process that allows that migration, is going to be essential in order to permit the upgrades to happen in a way that doesn't lose contact with the technologies they're leaving. We're well aware that a typical jurisdiction that made an investment 8 years ago in an analog system is not likely to be able to afford to spend $11 million or $20 million or $100 million to go to a digital system in the next year or 2 or 3 years. The technologies we deal with here, and the way public safety agencies put them into place, means that some of the systems will last 30 years, even though the technology life cycle is 18 to 24 months.

So all of our planning and all of our standards are designed to take this into account so we don't leave behind legacy systems. There will always be legacy systems with us.

Ms. MILLER. Mr. Chair, I don't think that answered my question on how the Federal Government is going to provide funding. Have we provided long term funding for these legacy systems to continue the upgrades?

Mr. BERES. The Department continues to request the approximately $4 billion in homeland security grant funds, of which upgrades for interoperability communications planning, the exercises that Dr. Boyd talked about, all of which are allowable costs. As we progress down this road of upgrading technologies and looking back and hanging on to legacy systems, the funding that is currently in the President's budget that's before Congress now provides for us to look forward to new technologies and increase better interoperable communications at that State and local level.

Mr. BOYD. It's also important to remember that more than 97 percent of the funding that goes out to the field, even for emergency communications, is provided by States and localities. Federal money represents only a relatively small part of that.

So one of the things first responders asked us to help them with was to provide them tools to build a business case that they could use to take to their county commissions, to their city councils and their State legislatures to explain why interoperability was important and why interoperability had to be built into new funding plans, and why you had to think about a life cycle system instead

of buying a system now and then hoping that it will last 30 years and then funding a whole new system in 30 years.

One of the things that we believe that a rationally developed set of standards will help us do is to allow incremental upgrades of technologies. Right now, one of the unfortunate problems we have, because of the lack of standards, is proprietary features and proprietary standards that make it very, very difficult for a community to upgrade pieces of a system in 2 or 3 years that are a little more advanced.

For example even though you may go buy a device for your computer that's designed to operate on a version 1.1 bus, it will work in your new computer with a version 2 bus. That's not the case with most of the communications systems now, because of proprietary elements. Typically, manufacturers will design a system and sell it for about 5 to 7 years, then manufacture parts for it for a few years and finally stop supporting it. Unfortunately, because we don't have the universal standards yet, that we're trying to put in place, when it comes time to modernize a system, agencies only have two choices: either continue to buy equipment with the current technology, which means going to the used market and hoping there somebody has recently retired a system that they can use for parts to maintain it; or it means buying an entirely new system, which usually means a bond issue.

Ms. MCCOLLUM. Well, thank you, Mr. Chair. As you can see, if we don't have a universal system out there, we are going to have many municipalities making a choice as to what to do, similar to just throwing a dart at a dart board and hoping it lands in the right space. So this really needs to be addressed.

Mr. PUTNAM. Thank you very much.

Mr. Muleta, you've heard your fellow panelists field these questions about the issues that are out there. Could you give us some sense of what concrete success we have had in improving interoperability since September 11, 2001?

Mr. MULETA. Given that there are 40,000 public safety licensees, it's difficult to find one concrete example. I think there are many. The bigger success has been all of the things that we are talking about today, which is the focus on long term planning, the focus on the need for interoperability outside of the sort of narrow context of urban areas, but to look at threat areas and sort of understand that it's all part of the matrix. I think there has just been an incredible amount of focus on those issues.

Other areas where I have seen success has been the way that the public safety community has come together in terms of representing their interests in front of FCC and making sure that we are focused on addressing interoperability issues. They are not sort of like small pockets of divided forces, so that the Commission can act in concert in dealing with these issues.

So for me, it's very difficult to say here are communities where it's very successful.

Mr. PUTNAM. Let me try to narrow it down a little bit, then.

Mr. MULETA. Let me address one community. Alexandria, the community of interest that follows along the Department of Defense Pentagon building, in Arlington, Alexandria, Fairfax County and the District have a workable system that actually worked on

September 11th by statements made by other folks. But they had a coordinated plan, they could react accordingly. They had the processes in place. That's a community that was already there. I think that reflects the sort of threat level that the Pentagon has as opposed to other communities out there.

Mr. PUTNAM. Thank you. We have a panelist from the area, too, in our second panel, so we'll be able to hear from them.

40,000 licensees, how many options are there? If you have municipality, local fire department puts out an RFP to upgrade their system, how many choices are there?

Mr. MULETA. By choices, in terms of systems?

Mr. PUTNAM. Yes.

Mr. MULETA. I think there are 10 different bands that can be used for public safety. So that at least gives you an idea of the size of the matrix, because the first thing that you do with a public safety system, you say, what channels are available for use. And depending on the sophistication of the licensee, what goes into it is, am I part of a statewide system, am I part of that plan, am I part of a regional plan, are there channels available and then what can I afford. Am I having to buy a used system, am I having to buy a new one, because the price difference is significant.

So I think in terms of technology, one of the issues has been to, and this is a broader statement than a spectrum issue, that there needs to be more variation, more ability, more technology available that's similar to the computer technology where you sort of have open standards and you can plug and play, and have different manufacturers playing in the field.

So there are lots of choices on how you design your systems, but probably not enough open systems to allow for the sort of mix and match, plug and play type of environment that we have in the computing world. I think we are in essence in the worst of best worlds, there are too many choices and not enough choices in other areas.

Mr. PUTNAM. So how many manufacturers are there that are in this field?

Mr. MULETA. I think it's sort of a handful of significant players in the field. A couple of companies have significant market share in the public safety community.

As Dr. Boyd explained, these systems are being purchased for sort of 10, 15 year life cycles. And the ability of companies to support that on a proprietary basis limits the universal appeal of this business. So it's limited. But we are trying to get into the world where you have plug and play.

Mr. PUTNAM. Dr. Boyd, let's pursue that a little bit. Coming out of the State legislature, we want a 6-year plan or something to get the highway patrol 800 megahertz trunk systems and undoubtedly by the time the last batch is purchased in year 6 the folks who got theirs in year 1 are already up onto something else.

Where does this really end? Is this just a cat chasing its tail? What is the end mission? The GAO is quoted as saying that you will never be fully interoperable, so what is, how do we define success and what is the best way to approach this? What is the ordinary emergency mission that we are using as sort of our model? And undoubtedly September 11th, I would hope is a bit on the outlier side of the spectrum, and tornadoes in the Midwest and

floods or hurricanes on the Gulf Coast or things like that would probably be the more normal type of multi-jurisdictional emergency.

How will we ever get our arms around this and how do we approach it? Do we approach it for what's best for a county, what's best for a State, what's best for a region? Help me understand that a little bit better, please.

Mr. BOYD. Let me do it in two parts. Our philosophy argues first that localities are not going to be able to use communications equipment effectively that they don't use in normal day to day emergencies. Our perspective is that emergencies are the business of public safety, that it's not just the major terrorist event or the hurricane. It is, in fact, what they do 24 hours a day, 7 days a week, year round.

So the issue then is scale. Can you handle the incident all the way from a massive terrorist attack in communications terms all the way down to something as small as a traffic stop? We maintain first that this needs to be communications equipment they're going to use all the time.

The second part is that we believe the development of a robust standards process, and trying Federal grants to implementation of guidance built around those standards is one of the ways to begin to move in the right direction and to encourage industry to move that way. In fact, if you had asked me that question in, let's say, 1980, about whether we're going to have that kind of issue with computers, I would have had to say that as things stood then, you had a choice of CPM, you had DOS, and a long list of other different kinds of operating systems, different networks and even different versions of ASCII, whether it was a proprietary IBM called EBCDIC or other kinds of digital exchange or digital storage mechanisms. It made it extraordinarily difficult to exchange information.

I think that as the standards came along, they were driven in large measure by the market, and large buyers like the Federal Government which said, well, gee, if we're going to buy these things they really need to come down to kind of common sorts of exchange protocols and operating systems and so on. I think the same thing is going to have to happen in communications. That's the way we're trying to approach things, to try to develop guidance first, because standards take a little while to produce to get everybody on board, because the law governs how standards are developed.

So we first want to go to guidance that says, look, as you build your statewide plans, you have to involve everybody in the statewide plan, beginning at the lowest level and bringing all levels in, or you will encounter, as Ms. Miller has pointed out, the kind of situation you have in some States where you have a statewide system that only the State police are on and nobody else is, because they didn't bring the localities in first.

We think that is the first step, that you have to get everybody working together along a common set of protocols and develop a common appreciation of why interoperability needs to be a part of common planning. Then you can begin to demand compliance as you develop your RFPs for new systems. You can demand a way

to ensure interoperability, even if in the early days it relies on a patch system, something like the kinds of patches that are used in the national capital region. This way you begin to force an increasing degree of interoperability so that you eventually arrive at what you're after.

You asked a minute ago whether there were certain communities that had already developed some reasonably successful interoperability solutions, and there are. They're not generally statewide, although South Dakota comes close to qualifying as a statewide solution. It may be a bit easier with a population of 650,000, but they actually have a statewide system where they helped to buy and put the systems in place for everybody.

There is a system in the State of Indiana which does not encompass the whole State, but nevertheless began by working with localities to help bring them in. San Diego County was probably the first real success for an area in the United States when they developed a fairly primitive, but effective solution by developing the first multi-jurisdictional set of governance agreements, protocols, standard operating procedures and exercises to allow interoperability in the county. They did this almost 10 years ago under a project that I was fortunate enough to be involved in while I was still in Justice.

You have a number of such exempts. The State of Virginia now has a statewide plan that actually starts at the lowest levels, and works its way all the way up to the Richmonds and the Northern Virginias in order to bring them all together in a statewide plan. So there is movement, but this is a big challenge. This is a large activity. There are, depending on how you count them, somewhere between 40,000 and 60,000 independent jurisdictions who have to be a part of bringing all this together.

Making that kind of change is going to take a while. But I think we've really laid a foundation and really attracted attention, in large measure, because Congress has applied so much attention and so much emphasis to interoperability over the past few years.

Mr. PUTNAM. Thank you.

Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. Muleta, do I understand correctly that the FCC relies mostly on volunteers from input and operations of public safety spectrums? And is the operation of public safety spectrum well funded, or is the use of volunteers due to a lack of resources?

Mr. MULETA. To be honest with you, I don't understand the context of the question. The FCC manages the spectrum for public safety in the sense that we make the allocation and then the assignment of that to public safety licensees, we award the licenses. There is no use of volunteers in that context.

There are State interoperability committees, regional planning committees that are composed of public safety officials who get together, based on requests from, as sort of representative licensees that develop plans, regional plans, statewide plans. I think the question might be referring to the fact that some of these, there's not a specific mandate from the FCC to require State interoperability committees. That's a recommendation that has been made by the National Coordination Committee that we established to

plan for the 700 megahertz, the use of the public safety band in 700 megahertz.

We are considering that option. I think one of the issues that we have to be careful about is when you mandate a specific requirement on States, on how they can deploy their resources, we want to make sure that we get all the input and sort of carefully deliberate that issue.

There's nothing to prevent States from actually putting together their own interoperability groups. So we believe there is enough grant resources and things like that to make this a viable approach.

Mr. CLAY. OK, so specifically you rejected, rather the FCC's rejection of the council's recommendation for a national planning committee's utilization of a data base for frequency coordination, that was rejected by FCC, correct?

Mr. MULETA. I think a recommendation was made to us. We have not acted on it. We're seeking comment and are thinking through the process of what the requirements would be on establishing a mandate on this States to do things in a particular way. So we're seeking comment on those and waiting to see if we can make a decision. I think we hope to have something on the various recommendations made by the National Coordination Committee, which was a Federal advisory committee that we established to plan for the 700 megahertz. They made a set of requirements. And I think we'll act upon them accordingly.

Mr. CLAY. And the FCC didn't necessarily care for the recommendations, so you rejected them and then you FE

Mr. MULETA. Again, I FE

Mr. CLAY. So then you will come out with a response to them at what date?

Mr. MULETA. I think the advisory board gave us a set of recommendations and we will review them as part of the normal FCC process. The commissioners will make choices on which issues can go forward and are appropriate responses. There is a set of recommendations made, but I think the Commission is reviewing them and planning to make decisions on them.

Mr. CLAY. Let me get to Mr. Boyd. Dr. Boyd, in terms of technology, can you identify for us any new technological advances that have the promise of improving interoperable communications among first responders, or spectrum issues holding back the emergence of new products?

Mr. BOYD. I'm not aware of any special issues that would hold back the emergence of new products. What I would say is that in the near term, there are two kinds of technologies out there, those that can address the issue in the near term and those that are more on the horizon. In the near term, technologies exist now that can help, especially to achieve command level interoperability.

These are largely switch systems, systems such as those produced by Raytheon, the ACU systems, the SiTech systems, and a number of others that you can think of as high-tech computer driven CAT systems that can tie one radio to another. These allow for interim, emergency based interoperability. It's not what we want ultimately, because it ties up a channel on each system, so it's spectrally inefficient, requiring twice as much spectrum.

On the horizon, though, we're seeing newer digital technologies coming into play, including radio-over IP, which is a way of using digital technologies to permit multiple networks to share the same spectrum as though they were on different channels, when in fact they are on the same channel. We are able to do this in part because voices can be digitized into very tiny packets. So you can put a great many in a single channel. There are experiments under way now.

A second possibility is software defined radio. The Defense Department has a major software defined radio effort underway called the Joint Tactical Radio System, which we're monitoring very closely. And there are some private companies that are working on software defined radios. These are radios that are computer driven so you can tell them to operate on whatever band you want them to operate on, using whatever wave form you want them to operate on—digital, analog or whatever—and you can drive this all out of a single box.

None of these are panaceas, but there are nevertheless technologies which we think are moving very rapidly into this field. In some respects, radio, even though it's an older technology, is 10 or 15 years behind the computer revolution. That's in part because installing these systems has been very expensive, so jurisdictions find it difficult to simply upgrade tomorrow with a new technology.

Mr. CLAY. Thank you for that response. Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you, Mr. Clay, and I regret that we're going to have to end the first panel here and seat the second panel. So we very much appreciate our first panel's comments. We look forward to hearing from the boots on the ground.

The subcommittee will recess for such time as it takes to seat panel No. 2.

[Recess.]

Mr. PUTNAM. I hate to do this to our witnesses who just sat down, but if you would please rise and raise your right hands for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. Note for the record that all the witnesses responded in the affirmative. We appreciate your being with us today and look forward to your testimony.

Our first witness to testify will be Maureen Lischke. Ms. Lischke is a member of the Senior Executive Service and has served as the National Guard Bureau Chief Information Officer since 1996. She also serves as the Deputy Director of Command Control Communications and Computers.

Prior to joining the National Guard Bureau as the Program Manager for the Reserve Component Automation System in 1994, Ms. Lischke worked for the Defense Communications Agency, now the Defense Information Systems Agency. She also served as the Deputy Director of Program Oversight with the Office of the Assistant Secretary of Defense for Command Control Communications and Intelligence. She has been recognized with a number of awards and recognitions, and she was among the 2002 Federal Computer Week top 100 executives recognized from Government, industry and aca-

demia who had the great impact on Government information systems for that year.

We welcome you to the subcommittee and look forward to your testimony. You are recognized for 5 minutes.

STATEMENT OF MAUREEN LISCHKE, SENIOR EXECUTIVE SERVICE, CHIEF INFORMATION OFFICER, NATIONAL GUARD BUREAU

Ms. LISCHKE. Thank you and good afternoon, Mr. Chairman and distinguished members of the subcommittee.

I would like to thank you for the opportunity to speak with you today on this very important matter. In the interest of time, I have prepared a written statement that I will submit for the record. But I would like to take several minutes to address several important points.

As you know, the National Guard lives with one foot in the Federal camp and one foot in the State camp. We are the one organization that is the bridge between Federal and State governments. We live in a world where we have to communicate with a myriad of organizations and therefore interoperability is very important to us.

At least 25 of our Adjutants General are also the State emergency management officials, and at least 15 of our Adjutants General have been named the senior homeland security advisor to the Governor. In order to better coordinate with all these different organizations, we have created standing joint force headquarters in each of the States, territories and the District of Columbia. We have representatives from each of the military branches and each of the Federal, State and local governments in those headquarters.

In order to address the need for better communications, we have with the strong support of Congress implemented a robust network that not only connects all of our armories together and our standing joint force headquarters, but also connects us to the Department of Defense and to our State networks. We have built 321 digitized facilities through our distributive training technology project that we are using for exercise training with our first responders as well as using them for command and control locations when the situation calls for it. In fact, they were invaluable to us right after September 11.

We also have fielded 32 civil support teams that have a communications band as part of their suite of equipment. This provides them with interagency communications. We currently have another 12 teams that are in training and are looking forward to receiving the resources to stand up the last 11 teams.

The recent GAO report referenced the Defense Science Board's summer study that came out in November of last year. In that summer study, the Defense Science Board captured the requirements of the States for communications. As a result, we have developed a concept that we refer to as the Joint CONUS Communications Support Environment. It's not a single program, but rather a number of different initiatives to address those States' requirements of interoperable communications down to the incident site, as well as being able to pass information up and down to those organizations that need it. It also provides for a joint operations cen-

ter in each of the 54 standing joint force headquarters that are being manned 24 hours a day, 7 days a week.

We are currently running several pilots to determine the solutions that will best meet the States' requirements. And in our development of the concept of the Joint CONUS Communications Support Environment, we have been working with David Boyd to ensure we are all going in the same direction.

Interoperable communications is critical to us, and we feel it is very important to establish a nationwide strategy. We see SAFECOM as that program that is addressing this, and we have been working with them to contribute to their success.

In summary, the National Guard is committed to providing interoperable communications working with Federal, State and local governments and using our unique status to contribute to the success in this endeavor.

I want to thank you for the opportunity to speak to you today and I look forward to your questions.

[The prepared statement of Ms. Lischke follows:]

RECORD VERSION

STATEMENT BY

MAUREEN T. LISCHKE
SENIOR EXECUTIVE SERVICE
CHIEF INFORMATION OFFICER, NATIONAL GUARD BUREAU

BEFORE THE

HOUSE GOVERNMENT REFORM COMMITTEE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

SECOND SESSION, 108TH CONGRESS

ON PROJECT SAFECOM: MORE TIME. MORE MONEY. MORE COMMUNICATION? WHAT PROGRESS HAVE WE MADE IN ACHIEVING INTEROPERABLE COMMUNICATION BETWEEN LOCAL, STATE, AND FEDERAL FIRST RESPONDERS?

SEPTEMBER 8, 2004

FOR OFFICIAL USE ONLY
UNTIL RELEASED BY
THE HOUSE GOVERNMENT REFORM COMMITTEE,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS

STATEMENT BY
MAUREEN T. LISCHKE
SENIOR EXECUTIVE SERVICE
CHIEF INFORMATION OFFICER, NATIONAL GUARD BUREAU

Good afternoon, Mr. Chairman and other distinguished members of this subcommittee. Thank you for inviting me to testify before you today to address the National Guard's existing ability to support first responders. I will also discuss information technology requirements that the National Guard of the several states have articulated for further enhancing their ability to support the first responders.

As you know, Section 10501, Title 10, United States Code provides the purpose of the National Guard Bureau to be the channel of communications between the Departments of the Army and Air Force and the several states on matters concerning the National Guard. In this regard, to assist in mobilization, training, and administration, the National Guard Bureau, with Congress' strong support, established a communications structure called "Guardnet." It links over 3,300 National Guard installations in over 2,700 communities in all 50 states, three territories, and the District of Columbia to the Department of Defense. Three hundred and twenty-one sites

are equipped with video teleconferencing equipment provided by the Distributive Training Technology Project that have been used during emergency operations for information sharing and for exercise training with first responders. In fact, sites in New York, New Jersey and Virginia were used for command and control, providing situational awareness and information sharing following 9/11. Since then, the National Guard has provided IT support for numerous events, to include the Winter Olympics in Utah, the G-8 Summit in June of this year, the Democratic National Convention in July, and just recently at the Republican National Convention in New York.

The National Guard is supporting the homeland security activities of the states. The National Guard Adjutants General in 25 states are dual-hatted as the Senior State Emergency Management Official reporting to the Governor. In 19 states the Adjutants General are cabinet level officials equal to the State Emergency Management Officer and there are various arrangements in the remaining states. Further, in 15 states the Adjutants General also serve as the Homeland Security advisor to the Governor. There is a National Guard Standing Joint Force Headquarters in each state and territory that consists of National Guard staff, as well as representatives from all of the military services and the federal, state, and local governments.

It is the National Guard who has the exclusive ability for exchange of classified information within the states.

In brief, the National Guard is presently integrated with both federal and state IT networks and can be called to participate with the first responders. The National Guard's close involvement with both state and federal governments provides a unique opportunity to assist in solving the problem of interoperability and information sharing.

In this regard, the National Guard Bureau is aggressively participating in exercises, demonstration projects, strategies, initiatives and programs, such as the Department of Homeland Security's SAFECOM program. We are working hard to improve interoperability and we recognize that all of our initiatives must be interoperable not only with Northern Command, but also with a federal government enterprise strategy. SAFECOM is the activity addressing this enterprise strategy and we are working to contribute to their success, thus assisting in the trusted sharing of information among all stakeholders involved in Homeland Security.

In 2001, the National Guard Bureau commissioned a Strategic Issues Task Force to determine IT training and

command, control and communication system support requirements for defense of the homeland. Based on a survey, the Task Force recommended a National Guard Joint Operations Center to serve as a single focal point for state, federal agency and DoD support requirements. Along with the Joint Operations Center there is a requirement to enhance Guardnet to be able to carry additional communication traffic between the state Joint Force Headquarters and the networks of DoD, the Military Departments and other federal and state agencies. The states require a quick reaction communications team at each state Joint Force Headquarters that can move quickly to any incident site. At the incident site, the states need wireless "reach-back" communications to the Emergency Operations Center and the federal and state networks. Within the incident site area, there is a need for interoperable communications among responders. Additionally, the states desire enhanced technologies in the distance learning classrooms to support homeland security training to serve as a forward Emergency Operations Center. Finally, there is a requirement for a National Guard communications unit trained and tasked to support any state when the state needs additional IT resources during a declared emergency. These requirements have been identified and are the focus of the National Guard Bureau.

In closing, the National Guard Bureau strongly concurs with the Chairman's remarks before this subcommittee in July that, "Information sharing and coordination among government organizations are central to producing comprehensive and practical approaches and solutions to combating threats." The National Guard Bureau is aware of its unique state and federal status under the Constitution and the opportunities that dual status brings to assisting in the war on terrorism. It is committed to providing interoperable information-sharing capabilities that are secure, reliable, dependable and that respect privacy provisions of the users.

Again, thank you for the opportunity to testify today. I look forward to your questions.

Mr. PUTNAM. Thank you very much. I'm sure there will be a number of them.

Our next witness is Vincent Stile. Mr. Stile is the past president of the Association of Public Safety Communications Officials International, Inc. He became involved with the APCO association when he began serving as southern New York State's assistant frequency coordinator for police and local government in 1970.

During his tenure with APCO, Mr. Stile served in a number of positions. He served on the APCO automated frequency coordination board of directors and on the task force that developed the first in-house automated frequency coordination system.

He is a 40 year veteran of the Suffolk County Police Department which he currently serves as the police radio communications director, a position he has held since 1985. He budgets, plans, designs and implements new wireless communications systems for the department, the 14th largest in the United States.

We are looking forward to your hands-on expertise. You are recognized for 5 minutes.

STATEMENT OF VINCENT STILE, PAST PRESIDENT, ASSOCIATION OF PUBLIC SAFETY COMMUNICATIONS OFFICIALS INTERNATIONAL, INC.

Mr. STILE. Thank you, Mr. Chairman.

As stated, I am Vincent Stile, and I'm a retired police officer from the Suffolk County Police Department and serving as a frequency radio coordinator and radio spectrum management counseling for police and local government of southern New York State. I presently also serve as vice chair of the Department of Homeland Security Project SAFECOM executive committee.

I am here today to discuss interoperability as it relates to public safety achievements toward that goal. I would first like to point out that the goals of interoperability are not new, and the term itself has taken on a heightened level of meaning since the attack on this Nation 3 years ago. Interoperability is a daily occurrence for first responders as they perform their routine duties. Interoperability first begins in our local communities as police officers, firemen, EMS workers, along with their 911 dispatchers, all first responders, communicate with each other.

As I pointed out in my written testimony, the APCO homeland security task force identified six topics that most identified the needs for putting together responsible interoperability planning. Recently, prior to the Republican National Convention in New York City, I brought together a number of public safety communication specialists from surrounding areas of New York City, including radio personnel from the New York City police department. I mention this to illustrate that the planning process that homeland security task force identified as steps to putting together a plan, it was important to have this kind of a meeting.

It is without question that the city planners and New York City police department and Secret Service all had all the communications concerns well covered for the city. The purpose of our meeting, of the surrounding area communications specialist, was to make plans in the event of a mutual aid that may be required from the surrounding police, fire and EMS agencies. We discussed what

radio channels would be in use to communicate on and who would be in control of designated radio assignments. This step represents the planning stage of Homeland Security Task Force recommendations.

We came together to plan what the action would be if necessary if we were called out. Any call for aid would represent the next step in the recommendations which was interoperability phase where radio communications would cross over the boundaries of official jurisdictions.

Next was the selection of radio frequencies that would work and provide coverage in that area. Servability and redundancy was built into the planning process as the communications specialists present all knew the range and coverage to expect from the selected radio channels, as well as what radio systems would be used or re-used for redundancy. And finally, the training portion of the task force recommendations occurred as part of the routine testing that has been conducted in the area up to this point.

The pre-planning of public safety entities is extremely important and has basically taken hold by many of the local government agencies due to the help that is beginning to come forward from the Federal funding sources and guidelines provided through the help of Federal information sources. Much of this help has been infused into the Federal programs by State and local government first responders who were sought after to provide input for what was necessary to plan for the interoperability.

The Federal guidelines initiated by the Department of Homeland Security SAFECOM program are structured to educate, train, provide financial assistance as money becomes available. These programs can be a complete source for guiding State and local government to develop interoperability planning.

Suffolk County and Nassau County in Long Island are developing a bi-county interoperability program with the help of Federal grants they recently both received. As part of this program, 800 megahertz national channel base stations will be located at vantage points on Long Island to provide radio coverage for first responders throughout most of Nassau and Suffolk Counties. The extension of these national channels will be functional in the five boroughs of New York City under the control of the Port Authority.

Also as part of this grant money, radios will be purchased to allow Suffolk County police officers that travel through Nassau County and into Manhattan have continued communications with a monitoring dispatcher at each end of the dispatch areas.

Interoperability programs such as those mentioned are also possible with the assistance of Federal funding and routine testing and training on the systems implemented plus ongoing upgrading of improved communications equipment. Clearly, however, if there is a lack of radio spectrum for public safety, all the planning for interoperability will only delay its implementation.

I want to thank you very much again for conducting these hearings and allowing me to appear before you today. APCO looks forward to working with Congress to assure that public safety agencies have access to the needed resources and spectrum that are needed to protect the lives and the property of the public we serve.

[The prepared statement of Mr. Stile follows:]

TESTIMONY OF

VINCENT R. STILE, PAST PRESIDENT

ASSOCIATION OF PUBLIC-SAFETY COMMUNICATIONS OFFICIALS-INTERNATIONAL, INC.

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

September 8, 2004

Thank you, Chairman Putnam and members of the committee. My name is Vincent Stile, and I submit this testimony today in my capacity as the immediate Past President of the Association of Public-Safety Communications Officials-International, Inc. (APCO), the nation's oldest and largest public safety communications organization. I am also the Police Radio Communications Systems Director for the Suffolk County Police Department, Long Island, New York, the fourteenth largest police department in the nation, and serve as chair of the New York Metropolitan Advisory Committee (NYMAC) dealing with the concerns of radio spectrum as it affects first responders in New York City and its surrounding areas. I also serve as Vice-chair of the Department of Homeland Security Project SAFECOM Executive Committee.

Founded in 1935, APCO has over 17,000 individual members, most of whom are state or local government employees who manage and operate communications systems for police, fire, emergency medical and other public safety agencies. APCO International is a member driven association of communications professionals that provides leadership; influences public safety communications decisions of government and industry; promotes professional development; and, fosters the development and use of technology for the benefit of the public. APCO is certified by the Federal Communications Commission (FCC) as a frequency coordinator for state and local government public safety licensees. APCO recommends frequency assignments for applicants seeking to add or expand their communications system, with the goals preventing harmful interference to critical operations, promoting interoperability, and maximizing spectrum efficiency. APCO's frequency department consists of a full-time staff and over 55 volunteer local frequency advisors throughout the United States. Until recently, I was the primary local frequency advisor for Southern New York, and continue to serve as an alternate advisor. APCO is also deeply involved in a wide range of policy issues of concern to state and local government public safety communications, including spectrum allocation and management, deployment of Enhanced 9-1-1 services, and funding for new communications networks and systems. APCO frequently participates in proceedings regarding these issues at the FCC, before Congress, and in the Executive Branch.

I would like to begin by saying interoperability is not a new issue for public safety. It did not come in to being after the tragic events of September 11th but rather it has and continues to be a constant challenge to public safety. Interoperability occurs every day in our line of work. Fire fighters, police officers and emergency personnel work closely with each other on nearly all emergencies and they need to know that their communications systems will not fail them when

they need it the most. With that being said, we in the public safety communications industry are well aware of the limitations there are in establishing an interoperable communications system.

Unfortunately, some believe that such a system can be developed from a top down model, where the federal government identifies the solutions to interoperability and mandates these solutions to the local communities. I am here to tell you that this will not work. Emergencies happen at the local level. The first responders that are on the scene minutes after the incident has occurred are the local police, fire and emergency personal. The first 9-1-1 calls come in to the local public safety answering points and the first emergency personnel are dispatched from local emergency communications centers. Many times State and Federal assistance does not arrive until hours and sometimes days later. Most often the communications problems that occurred at the time of the incident have been fixed by the time State and Federal assistance is on the scene.

So what is needed? What can the Federal government do that is not already being done by local governments? How can the Federal government assist local governments to establish interoperable communications systems?

The answer involves planning, resources, funding and training. The solutions are very complex and many times very expensive. APCO's Homeland Security Task Force concluded that the following six broad topics encompass most of the needs identified following the tragic events of September 11th:

- **Planning:** establishing concise and mutually agreed upon methodology to respond to natural disasters and large scale terrorist actions that include chemical, biological and or nuclear threats.

- **Interoperability:** the ability of different government agencies or first responders (law enforcement, EMS, fire fighters) to communicate within and across departmental jurisdictional boundaries.

- **Radio Spectrum**: having sufficient spectrum for unfettered and high-quality reliable communications in emergency situations.

- **Survivability/Redundancy:** knowing how to plan and having the funding available to build public safety communications systems and communication centers that can withstand a terrorist attack or other significant manmade and natural threats.

- **Security:** instigating processes and procedures to assure that public safety communications systems, centers and staff are protected with substantially increased security to thwart attempts by enemies of the United States to disrupt and destroy our emergency communication capability.

- **Personnel/Training:** providing the necessary training to public safety communications personnel to enable them to plan for any type of terrorist event, to utilize new technology, to be aware of new security systems and procedures, and to deal with the stresses associated with working in an environment characterized by perpetual anticipation.

After the events of September 11th, many communication centers moved quickly to update their emergency response plans, both at the agency and regional level. They found that those emergency management programs that had been on hold or scheduled for long-term development were now pushed to the top of the priority list. The pressure was on to assure the public that public safety communicators were prepared to answer the call in any situation – regardless of how remote a possibility. At the same time, elected officials wanted assurances that their communication centers could handle responding to new threats.

The federal government should be closely involved in assisting local communities to develop regional interoperability plans. The process needs to include many of the key personnel that would respond to a catastrophic event, which might include local police, fire, and emergency personnel as well as state and federal officials. It is without a doubt the best people to establish a regional interoperable plan are the local emergency personnel. They know their citizens, terrain, and resources. For example, I chair the New York Metropolitan Advisory Committee (NYMAC) which helps to coordinate the communications needs of the many public safety agencies serving New York City and nearby areas. Just last week, the NYMAC held a meeting with other regional emergency coordinators from New York and New Jersey. The purpose of the meeting was to identify procedures to follow for emergency communications during the Republican National Convention that may require mutual aid from the surrounding police, fire or EMS jurisdictions. Many APCO members are involved in similar regional efforts across the country on a on going basis.

Without adequate planning there can be little interoperability. APCO's Homeland Security Task Force identified three levels of interoperability planning.

- Day-to-day interoperability covers routine public safety operations, such as responding to a building fire that requires backup from a neighboring fire department, or a vehicle chase that crosses between towns.

- Mutual aid interoperability supports a joint and immediate response to catastrophic accidents, large scale incidents and natural disasters. It supports tactical communications in response to airplane crashes, bombings, forest fires, earthquakes, hurricanes and similar events that occur without warning.

- Task force interoperability supports local, state, and federal agencies collaborating for an extended period of time to address a particular problem. For example, a task force might lead extended recovery operations, provide security for major events, or respond to prolonged criminal activity. These are activities that are planned in advance.

However, planning is not enough. Public safety needs the resources to accomplish the goals they identify in the planning process. One of the scarcest resources that are needed by public safety is spectrum. Today APCO International is also testifying at the Senate Commerce, Science and Transportation committee hearing on one of the critical recommendations of the 9/11 Commission that Congress adopt pending legislation to clear broadcast stations from the 700 MHz band, portions of which have already been reallocated for public safety. APCO supports the HERO Act (H.R. 1425) introduced by Representatives Jane Harman and Curt Weldon in March 2003, establishing January 1, 2007, as a date certain for the clearing of these channels by the broadcasters. The passage of this act or a similar act is long overdue. The

ability of public safety to use this spectrum will go along way in establishing new and enhancing existing interoperable communications systems.

Many communities lack the spectrum required to establish an interoperable radio communications system. For example, without excess channel capacity, regional public safety agencies cannot dedicate sufficient channels for mutual aid or interoperability. Moreover, the lack of available radio spectrum has forced public safety agencies to operate in multiple, incompatible portions of the radio spectrum. With sufficient channel capacity, agencies within the same region could migrate to a spectrum efficient wide-area system operating in single frequency band.

As an example of the diverse spectrum use that now exists, the Suffolk County Police Department operates on 800 MHz band frequencies while fire, EMS, and some local police departments within the County's borders operate on either VHF (150-170 MHz) or UHF (450-512 MHz) band frequencies. Similar variations occur in neighboring Nassau County, and within New York City. The agencies in question are working hard to find ways to interoperate as best they can, but the lack of radio spectrum is a major hindrance. There are not even enough channels to create a cross-band patch, let alone sufficient spectrum for a wide-area, multi-agency system in a single frequency band. This is a common problem in many areas of the country.

Apart from interoperability, the lack of sufficient radio spectrum also limits internal communications capability for many public safety agencies. In many areas, existing channels are overcrowded just with internal communication, without even considering the need for "external"

interoperability. Many agencies are also unable to implement new state-of-the-art communication tools within existing, inadequate radio spectrum allocations.

Another resource that is greatly needed in establishing an interoperable communications system is funding. Many communities lack the funds needed to upgrade their current systems to new technological advances in communications equipment. After the planning process local communities need to be able to fund the programs and equipment that are identified in their plans. If there is not enough funding the best plans may never get implemented. However, funding can not be limited to one size fits all solutions. Several times we have been asked, what would be the cost of establishing a national interoperable communications system. We don't know. Each community has different needs and different funding sources to meet those needs. However, we do know that federal assistance is needed in funding many of the interoperable plans around the country. However, this assistance should not be tied a national model.

Tied closely to funding is the lack of new technologically advanced communications equipment. This has been an ongoing issue for many public safety communicators. At a time of national threat, technology that has been solely created for government use should be shared among the nations' first responders. Funding to pursue new technologies like software-defined radios should be provided. As part of their ongoing planning, public safety communicators should identify and reach out to known research centers and labs for information on the newest technology. Incompatible radio equipment from different vendors can also be a problem, especially in a digital environment. APCO anticipated this issue back in late 1980's, when it initiated Project 25 to establish user-driven, public safety digital interoperability standards. Those standards are now in use at the federal, state, and local levels, with digital, interoperable

Project 25 compatible radio equipment available from multiple vendors. Project 25 continues to refine and adapt standards to reflect improvement in technology and spectrum efficiency. Long term, technologies such as software defined radios may take interoperable equipment a step further, and APCO has been involved in that process through the National Public Safety Telecommunications Council.

I would like to conclude my testimony by impressing the need for training of public safety personnel. Some of the most important training that needs to occur to prepare public safety communicators for Homeland Security starts with the dispatchers and call-takers. It is critical that these individuals receive training in critical analysis of information to be able to spot an escalating incident. Dispatchers need additional information since they might be put in the role of helping to locate triage and evacuation areas.

To recap, what can the federal government do that is not already being done by the local governments and how can the federal government assist local governments in establishing interoperable communications systems? In short, the Department of Homeland Security SAFECOM Program should be given discretion to fund and promote a variety of interoperability approaches that meet specific local requirements.

On behalf of APCO International, I want to thank you once again for conducting this hearing and for allowing me to submit my testimony today. APCO looks forward to working with Congress to ensure that public safety agencies have the resources necessary to fulfill their obligation to protect the safety of life, health, and property.

Mr. PUTNAM. Thank you very much, Mr. Stile. We appreciate that.

Our next witness is Michael Neuhard. Chief Neuhard is a 27 year veteran of the Fairfax County Fire and Rescue Department, where he currently serves as the fire chief and Fairfax County Fire Marshal. In this position, he directs a staff of more than 1,400, including 1,200 uniformed personnel.

Chief Neuhard plans, coordinate and directs the overall operation of the fire and rescue department, including fire suppression, hazardous material abatement, emergency medical services, fire prevention, technical rescue and administrative and support services. He is a graduate of Mary Washington College and the University of Virginia's Weldon Cooper Center for Public Service Senior Executive Institute.

Chief Neuhard's professional affiliations include the Virginia State Fire Chiefs Association, the International Association of Firefighters and the International Association of Fire Chiefs.

Welcome to the subcommittee, sir, you are recognized for 5 minutes.

STATEMENT OF MICHAEL P. NEUHARD, FIRE CHIEF, FAIRFAX COUNTY FIRE AND RESCUE DEPARTMENT

Chief NEUHARD. Thank you, Mr. Chairman and distinguished members of the subcommittee. We are grateful for this opportunity to provide you with a local perspective on interoperability.

I have provided you with a complete, detailed set of comments and I will summarize some of those here today for you in my verbal comments.

I'd like to take a moment, Mr. Chairman, to indicate to you that our thoughts and concerns are with your first responders and citizens in Florida. We know what it's like to live through a disaster, and we know what they're going through now. And we hope that second storm doesn't come to you like it's scheduled to.

The Fairfax County Fire and Rescue Department serves over 1 million residents, workers and visitors each day in Fairfax County. We are an all hazards fire department, providing fire suppression efforts, basic life support and advanced life support emergency medical services and technical specialties, including rescue and cave-in capabilities, hazardous materials response and mitigation, and marine operations. Last year, we responded to over 90,000 calls for service and our call volume continues to grow.

Many of you know us because of our Fairfax County Urban Search and Rescue Program, which is renowned throughout the United States and the world, having responded to tragedies such as the bombing of the Murrah Building in Oklahoma City in 1995, and the Pentagon on September 11, 2001.

Interoperability is a critical issue for emergency responders. From a local perspective, where you are in this country will determine how successful you have been in achieving interoperability. It must be remembered that interoperability is not just about technology. In fact, it has been said that interoperability is really 80 percent communications and coordination in various forms and only 20 percent technical.

Critical components of emergency response systems which should be interoperable but are not necessarily technical in nature including common incident management techniques, common terminology, common policy and procedures, standardized training, compatible equipment, such as protective clothing, metering devices, self contained breathing apparatus and redundant methods of communication. While it is important to continue to improve upon and advance technical interoperability amongst wireless communication devices, it must be remembered that they will be useless, confusing and counterproductive if adequate attention is not given to emergency response systems as a whole in those areas that I've just mentioned.

The Commonwealth of Virginia partnered with SAFECOM to design a locally driven planning approach to enhance communications interoperability across Virginia.

Mr. PUTNAM. If you want to just, well, by the time I got around to letting you wait, they quit on us. Please proceed.

Chief NEUHARD. Thank you. I was mentioning the partnership between the State of Virginia and SAFECOM at the time and their efforts to enhance communication interoperability across the Commonwealth, which has ultimately resulted in a strategic plan that we are now implementing. The process included six regional focus group sessions to capture perspective from local public safety responders throughout the Commonwealth. Key strategic goals include expanding the statewide use of common language and coordinated communication protocols, increasing interoperability capabilities and coordination by maximizing the use of existing communications systems and equipment, and by planning for future technology purchases.

Also, we are attempting to enhance the knowledge of proper use of communications equipment by providing frequent and routine training for public safety personnel. The plan is now being implemented by a full time program manager known as the Commonwealth interoperability coordinator.

There are many challenges that remain. We still face the challenge of our computer aided dispatch systems talking to each other within a region. The capability is necessary so that we can effectively transmit through existing systems amongst jurisdictions written information and dated field units.

We still have a long way to go to assure that there is adequate and common command processes, common language and policies and procedures that ensure seamless functioning on an emergency scene between multiple agencies. Many localities continue to simply buy new radios, some through Federal grants, without having the proper training on operation and integration of that equipment into emergency operations. Exercises of new equipment and procedures at the regional level is still very uncommon. We need to support more regional training and exercises to incorporate interoperability solutions and identify additional gaps.

The Department of Homeland Security, through the SAFECOM program, has gained the support of all the major associations representing public safety officials, State and local elected and appointed officials. In January 2004, the 10 associations released a joint statement that declared, with the advent of the SAFECOM

program, public safety, State and local government finally have a voice in public safety discussions at the Federal level and confident that the Government is coordinating its resources.

In conclusion, the key to all interoperability is cooperation among and between the various agencies and jurisdictions. Maintaining forward momentum on improving communications and operational interoperability requires continued actions on multiple fronts, including common command language, local and State level planning, common policy and procedures, training and technical advances. It is imperative that interoperability remain a high priority at all levels of Government and with adequate funding, coordination and support. Failure to do so will allow interoperability to be a passing fad leading to inefficiencies and poor performance at the next major emergency requiring more than one agency to respond or more than one level of Government.

Project SAFECOM is one answer to ensuring it stays focused at the Federal level. Thank you very much.

[NOTE.—The Commonwealth of Virginia report entitled, "Strategic Plan for Statewide Communications Interoperability, Fiscal Years 2005–2007," may be found in subcommittee files.]

[The prepared statement of Chief Neuhard follows:]

Interoperability: A Local Perspective

Testimony by Chief Michael P. Neuhard
Fairfax County Fire and Rescue Department
before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Wednesday, September 8, 2004

Introduction

Chairman Putnam, distinguished members of the Subcommittee, my name is Michael P. Neuhard, and I am the Fire Chief for the Fairfax County Fire and Rescue Department located in the Northern Virginia area and a member of the International Association of Fire Chiefs. Thank you for the opportunity to provide you with a local perspective on Project SAFECOM and the issues of interoperability.

The Fairfax County Fire and Rescue Department serves over one million residents, as well as workers in local businesses and industry, and transient visitors who pass through our jurisdiction on one of the interstate highways that traverse our County. We provide emergency service through a network of 35 strategically placed fire stations and a staff of over 1400 dedicated men and women. Our stations are staffed 24 hours a day, 7 days a week, and 365 days a year. We are an all-hazard fire department, providing fire suppression efforts, basic life support (BLS) and advanced life support (ALS) emergency medical services, and technical specialties to include specialized rescue and cave-in capabilities, hazardous materials response and mitigation and marine operations. The Department also provides fire and hazardous materials preventative services through its Fire Marshal's Office. Last year, we responded to over 90,000 calls for service and our call volume continues to grow.

Many of you know of us because Fairfax County's Urban Search and Rescue (US&R) program is renowned throughout the United States as one of the premier FEMA-supported specialty units. We are a premier leader in training, readiness, response and recovery, in catastrophic event mitigation. We have responded to tragedies such as the bombing of the Murrah building in Oklahoma City on April 19, 1995, and the Pentagon on September 11, 2001. The team is recognized through the grant support from the Office of Foreign Disaster Assistance (OFDA) to respond to disasters, either man-made or natural, through-out the world. Our team has traveled to and assisted in the Armenia Earthquake in 1988, the Philippines Earthquake in 1990, the Nairobi Kenya U.S. Embassy Bombing in 1998, the Izmit Turkey Earthquake, the Taiwan Earthquake, and the Duzce Turkey Earthquake in 1999.

I provide you with this information as background for a sense of the depth and scope of the services provided in a large urban area that has benefited from the efforts of regional cooperation and coordination. We continue to work toward achieving interoperability among our diverse jurisdictions in Northern Virginia and the Metropolitan Washington region. In addition, because of our proximity to Washington DC and the potential targets this area presents, we have been fortunate enough to receive Federal

funding support toward our goals of planning, preparedness, response, and mitigation activities.

Interoperability Overview

Interoperability is a critical issue for the emergency services – police, fire, and emergency management. From a local perspective, where you are in this country will determine how successful you have been in achieving interoperability. It must be remembered that interoperability is not just about technology. In fact, it has been said that interoperability is really 80 percent communication and coordination in various forms, and only 20 percent technical.

Critical components of emergency response systems which are interoperable, but not technical, include:

- common incident management techniques
- common terminology
- common policy and procedures
- standardized training
- compatible equipment such as protective clothing, metering devices, self-contained breathing apparatus
- common hose threads for firefighting, and
- redundant methods of communications

While it is important to continue to improve upon and advance technical interoperability amongst wireless communication devices, it must be remembered that they will be useless, confusing, and counter productive if adequate attention is not given to the emergency response system as a whole in those areas that I have just identified.

I would like to take the next few minutes to discuss three areas related to interoperability. They include what is happening at the state and local level in Virginia regarding interoperability, the challenges that continue to exist that must be overcome, and finally a local perspective on Project SAFECOM.

State and Local Perspective

The Commonwealth of Virginia partnered with SAFECOM, a federal program managed by the Department of Homeland Security, to design a locally-driven planning approach to enhance communications interoperability across Virginia that has resulted in a Commonwealth-wide strategic plan.

The locally-driven strategic planning process designed and employed by the Commonwealth and SAFECOM included six regional focus group sessions and a strategic planning session. The purpose of the regional focus group sessions was to capture perspectives from local public safety responders throughout the Commonwealth as the basis for the mission, vision, and initiatives presented at the strategic planning session. The outcome of the subsequent strategic planning session was consensus on

the mission, vision, and recommended key initiatives, all supported by data gathered from the regional focus group sessions.

Key strategic goals include the following:

- establish communications interoperability as a high priority
- expand the statewide use of a common language and coordinated communication protocols
- increase interoperability capabilities and coordination by maximizing the use of existing communications systems and equipment and by planning for future technology purchases, and
- enhance the knowledge and proper use of existing and future communications equipment by providing frequent and routine training for public safety personnel.[1]

This plan is now being implemented by a full time program manager known as the Commonwealth Interoperability Coordinator whose mission is to improve public safety in the Commonwealth through enhanced data and voice communications interoperability between local, regional, state, and federal agencies.

Challenges

There are many challenges that remain. While progress is being made on the technical sides of producing and having available radio communication that are interoperable, we still face the challenge of our computer aided dispatch systems talking to each other within a region. This capability is necessary so that we can effectively transmit through existing systems written information and data to field units.

We still have a long way to go to ensure that there is adequate and common command processes, common language, and policies and procedures that ensure seamless functioning on an emergency scene between multiple agencies.

Most federal grants have been specifically designed to authorize the purchase of equipment, yet the grants do not allow for planning and training expenses. The result is that many localities simply buy new radios without having the proper training on operation and integration of that equipment into emergency operations. In fact, it has also resulted in the purchase of the wrong equipment due to the lack of planning and study prior to purchasing.

While in Virginia interoperability is high on the priority list as demonstrated by the strategic plan and actions at the state and local level, conducting actual exercises of new equipment and procedures at the regional level is still very uncommon. We need

---

[1] Commonwealth of Virginia, *Strategic Plan for Statewide Communications Interoperability, Fiscal Years 2005-2007*

to support more regional training and exercises to incorporate interoperability solutions and identify additional gaps.

In summary, there is a lack of life-cycle planning. There continues to be technical barriers; there is a lack of information sharing and an inadequate level of training. These factors continue to be challenges towards the goal of interoperability. While much progress has been made on identifying the problems, we still have considerable work to do.

Project SAFECOM

The Department of Homeland Security, through the SAFECOM Program, has gained the support of all the major associations representing public safety officials (law enforcement, fire, and public safety communicators), state and local elected and appointed officials. In January 2004, the ten associations released a joint statement that declared "With the advent of the SAFECOM program ... public safety, state and local government finally have both a voice in public safety discussions at the federal level and confidence that the government is coordinating its resources."

The foundation of the SAFECOM Program and the driving force behind it has been the support of the local and state public safety practitioners. As a practitioner driven program, SAFECOM is a program designed by public safety for public safety creating interoperability solutions that are driven from the bottom-up.

Key accomplishments include $150 million in grants last year from FEMA and COPS; the completion of the Statement of Requirements; coordination of federal interoperability efforts; development of a methodology for statewide interoperability plans; and success of the RapidCom Initiative.[2]

Conclusion

The key to all interoperability is cooperation among and between the various agencies and jurisdictions. Maintaining forward momentum on improving communications and operational interoperability requires continued actions on multiple fronts, including common command language, local and state level planning, common policy and procedures, training, and technical advances. It is imperative that interoperability remains a high priority at the local, state, and federal levels with adequate funding, coordination, and support. Failure to do so will allow interoperability to be a passing fad leading to inefficiencies and poor performance at the next major emergency requiring more than one agency or level of government response. Project SAFECOM is one answer to ensuring it stays focused at the federal level.

Thank you very much.

---

[2] International Association of Fire Chiefs, Notes on Interoperability

Mr. PUTNAM. Thank you very much, Chief.

We have three votes pending, one, the clock is running now. Mr. Worden, we are going to move to your testimony, we will hold people here. We are going to do a very brief, brief round of questions. I certainly respect and appreciate the distance you all have traveled and your time being here with us, but unfortunately, we are going to have to cut the second panel short to get to the vote.

So Mr. Worden, your introduction, Chief of Telecommunications Branch of the Governor's Office of Emergency Services in California, the office responsible for providing a communications structure for daily operation of the agency. Mr. Worden is a 30 year veteran of the Air Force, where he commanded airlift control flight responsible for deploying communications and a support group directing communications information technology and other support services.

We greatly appreciate your being here, and you are recognized, sir, for 5 minutes.

STATEMENT OF THOMAS B. WORDEN, CHIEF, TELECOMMUNICATIONS BRANCH, STATE OF CALIFORNIA, GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Mr. WORDEN. Thank you, Mr. Chairman, and committee members.

I'll attempt to avoid repeating much that is in the prepared testimony, skim through here and just hit some highlights, and some highlights as well observed in the earlier testimony. My perspective is different. At the State level, the Office of Emergency Services, we focus on bringing public safety professional together across levels of government and across disciplines to do planning and to effectively use our statewide emergency management system to coordinate during emergencies.

We also do operate as the operator of public safety radio systems and administer the licenses of several statewide families of channels, bringing together public safety professionals from across the State, representing the different regions, the different geographics, the different disciplines and the different political and financial capabilities of the governments they represent.

The plans they wrote have served for decades, and they have been the model for planning. In the fire services they have risen to the level of doctrine that drives training and equipment decisions, not only in California but nationwide. That doctrine is what made the 1,000 vehicle deployment during the southern California firestorm possible. While we did have some difficulties, we responded to seven major incidents and only on a few did we have issues.

The worst issues were not, however, in San Diego County. The limited ability of the San Diego County system to respond in growing areas reflects more the lack of guidelines, established, accepted, if you will, standards, on how quickly you must expand your radio systems as communities develop in the suburban fringe and in the wildland urban interface. We have very well established standards by which we judge how soon we have to open a firehouse, how many police cars we need to add, but we do not have those standards in how many radio transmitters we have to add, how many repeaters, how much more complex to make the system, and yes,

we did have tremendous problems with calls crashing in the suburban and rural portions of San Diego County as a result of that lack of standards.

Project SAFECOM, by the way, has demonstrated the understanding that we build all of these programs successfully up from the local requirement to the region, to the State, and ultimately to some national standards.

Our most successful regional public safety radio systems, including San Diego, developed out of a need to resolve communications issues at the local level, lack of spectrum being one driver, the need to modernize extremely outdated equipment, and finding a funding mechanism to do so being the other. Again, when cross discipline committees have come together and cross government committees have come together, they have come up with the best solutions. We have yet to see a solution imposed from above which has been effectively implemented.

As the Chief said, technology is a very small part of the problem. I often tell people that given a reasonable amount of time and a huge amount of money, my communications specialists can get anybody to talk to anybody. But during a crisis, you don't have the time, and in government, we never have an unreasonable amount of money.

There has been a resistance, however, in the pervious grant programs to deal with the kind of detailed operational planning and technical analysis that the Chief and others have discussed. It's been resisted as time consuming; it's been resisted as frustrating. It is both of those, but it is the core of success.

We have been working with SAFECOM on RAPIDCom 9/30 and we've had the opportunity to read the progress reports from all 10 cities. Interestingly, we in California asked SAFECOM and the ICTAP team to focus on governance documents, on coming up with the words and phrases that will regulate how the shared frequency system will work.

We read reports from other cities that are still talking about who should be coming to the table to discuss who should be on the system. We're beyond that, but we're beyond that because in both cities, local government was already beyond that, not because of anything that was imposed on them.

Training is a huge issue. These are complex systems, even the ones fielded now. And if the public safety responder does not use those features in exercises, doesn't use them in daily operations, they will not use them effectively during crisis. Most of our grant programs have only now begun to address training as an essential portion of implementing these systems.

Funding, we've already talked about the difficulties for local government in retroactive funding and the need to resolve that. We do need process controls to make sure that the money is spent well, but we can protect, I think, local coffers as well as State coffers by assuming honesty as we develop our programs, rather than assuming dishonesty on the part of local government.

Another area of funding is those joint power authorities that Ms. McCollum referenced. Often, they require local governments to precommit to year in-year out funding. And when Federal and State

partners are not willing to do so, it's very difficult for those to go forward.

Very quickly, there are two other areas where Federal issues arise. We are happy to invite the tribal governments, but when they are unable to sign documents because of liability issues in those documents or issues that hit upon tribal sovereignty, we at State and local or regional committees cannot address those issues. And whether it's implementing the 800 megahertz consensus solution or other issues, we cannot deal with international border issues, which severely limit our ability to update in Southern California.

And with that, sir, I ran very quickly through. Thank you for your time, and we all stand ready for your questions.

[The prepared statement of Mr. Worden follows:]

STATEMENT OF THOMAS B. WORDEN
CHIEF, TELECOMMUNICATIONS BRANCH
STATE OF CALIFORNIA, GOVERNOR'S OFFICE OF EMERGENCY SERVICES
Before the
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS
September 8, 2004

Good afternoon, Mr. Chairman and distinguished members of the Subcommittee. I wish to thank you for the opportunity to speak before your subcommittee today.

I come to you with a somewhat different perspective than most of the other witnesses you are hearing today. As Chief of the Telecommunications Branch of the Governor's Office of Emergency Services for the State of California, I approach issues first as part of the State agency charged with coordinating California's planning for, response to, and recovery from emergencies. We focus significant effort on bringing public safety professionals together from all levels of government. We also operate several public safety radio systems and administer the licenses of several statewide families of channels.

California is proud of its long-standing success in developing both single discipline mutual aid radio systems and cross discipline systems, and in both cases developing approaches to both local and statewide use. These systems were built up by teams of public safety professionals, both operators and technicians who shared experience from the various regions of the state. Their diverse backgrounds helped to develop plans that have met the test of time. When we considered discussing those plans in this forum, we wondered if the old signature dates on these plans would cause readers to discount their value. It is in reality those dates that trumpet their value.

These teams of experts brought together:

- Urban, suburban, and rural communities;
- Coastal, foothill, valley, and alpine environments;
- City, county, special district, regional, state, Federal, and sometimes tribal organizations; and
- Management, dispatch, response, and communications technical personnel.

The plans that they wrote have served for decades, and in fact are the national interoperability models for two major FCC efforts, the Public Safety Wireless Advisory Committee and the 700 MHz National Coordination Committee. In the Fire Services these plans have risen to the level of doctrine that drives training and equipping decisions not only in California, but nationwide. These plans also provided part of the foundation that has enabled us in cooperation with the SAFECOM Program to implement the objectives of the RapidCom9/30 project to ensure the availability of command level interoperability within one hour at an incident site in San Francisco and Los Angeles by the end of September. As I go through my remarks I will continue to refer to this project and the SAFECOM Program's approach to it as an example of where

they are today and how local – state – Federal partnerships can achieve results that are both valid and rapid.

Under DHS, the SAFECOM Program has been configured properly to build upon the fact that interoperability is locally driven, from the bottom up. As evidenced by their "Statement of Requirements" document released this last spring, and their recently released (and practitioner developed) Interoperability Continuum chart that is attached to my written testimony, SAFECOM understands the complexities of interoperability. The coordination needed to achieve interoperability is not something that can be mandated from the Federal level, or even the state or regional level. Local officials already have the wealth of knowledge of the challenges they face. These challenges vary widely. What is a critical stumbling block to one area may be an engineering footnote in another.

The issues include:

- The hazard environment (weather, hazardous materials, sources of crime, and other dangerous conditions),
- The organizational environment (overlapping jurisdictions in the same discipline, dissimilar responsibility areas across disciplines, operational doctrines and practices, levels of training, and existing multi-agency or regional partnerships),
- The political environment (diversity of jurisdictions, relative wealth or tax base of jurisdictions, existing political partnerships, and pressures from regional, state, and Federal agencies), and finally
- The signal environment (geography, weather, competing signal sources, and the variety of density and types of development)

In California we have seen the development of very successful regional public safety systems often built around the need to resolve communications issues. These partnerships invested major efforts in determining how, when, and why the participants needed to talk to one another long before they started buying equipment. These discussions of communications issues drove discussions of operational issues. From the design of a "pursuit channel" among neighboring jurisdictions to the development of a command level coordination net, the operational requirement drove the technical solution. The RapidCom9/30 project found both California cities well on their way to implementing the technology. Both cities had hosted several testing operations to examine the use of interoperability gateways to enhance already existing operational partnerships.

Technology is only a small part of the interoperability solution. With the notable recent introduction of the Interoperable Communications Technical Assistance Program within ODP's UASI grants, Federal programs to provide communications equipment under the WMD or Homeland Security umbrella have generally ignored the requirement to develop operational procedures and governance <u>before</u> equipment is procured and installed. Planning, the type of detailed operational and technical analysis I am discussing here, seems to be resisted as too time consuming and frustrating. It is both. In many cases, these funding programs have asked for evidence of such planning, but will not fund the planning effort as a component of resolving the problem. Further, when they do call for the existence of a plan they contain little or no guidance on what constitutes a valid plan and who can help the applicant achieve that goal. Current

Federal funding cycles do not allow for stable planning environments in state and local entities. The time from grant announcement to grant guidance to funding commitment through procurement to reimbursement assumes a well-developed idea of the requirement and solution before the "approved purchase list" for the grant cycle is announced. In too many instances jurisdictions adopt solutions on the list because they are on the list, not because they were selected in a valid planning process. Manufacturers are quick to tout how their solution meets the requirements of one or more paragraphs in the grant guidance and their ability to deliver and invoice within the grant cycle. The SAFECOM Program personnel who have been working with our mostly local partners in RapidCom9/30 have devoted a good part of their efforts to the governance documents that will prescribe when, why, how, and by whom the interoperability systems will be employed. These documents are the outgrowth of a well-developed planning process. We have asked them to focus on developing governing document language in the two cities that is similar enough in its format and style to serve as a model for other regions as well.

Training is as large an issue as planning. Every first responder trains regularly on the specialized tools of his or her trade (weapons, fire fighting tools, vehicle operations, etc.), but the vast majority of first responders do not receive ongoing training on how to use communications systems. More importantly, in daily operations and training exercises they rarely get to use the advanced features that may be engineered in to their systems to ensure that they are able to use them in crisis. An airline pilot endures two grueling training cycles in the simulator each year to ingrain the proper use of the emergency features of the aircraft and to learn the symptoms of system failure. Unless the need and the technique are included in realistic training, first responders may well forget during a crisis that a certain knob position or button push enables them to make a distress call on a channel that all will hear. Several cycles of the main funding programs specifically excluded training. SAFECOM Program's approach to the RapidCom9/30 accelerated process has include the need to demonstrate the solution in a realistic, scenario-driven exercise environment where users can experience the effect of the system on their decision processes as well as hear the actual sharing of signals occur.

Having talked about planning and having talked about training, we come back to the issue of funding. Two issues bear attention. First, requiring state and local entities to expend their funds on the promise of being reimbursed is disruptive to ongoing local programs. For many jurisdictions these Federally supported investments represent a very large proportion of their discretionary budget. Anyone who has served long in a capacity to manage government budgets knows that the large majority of each year's expenditures is resistant, if not immune, to management. Federal grant guidance prohibits either advancing funds to sub-grantees for expenses, or providing a direct payment system for the invoices that they present. The result is that some other expenditure, not related to the grant, may have to be postponed until the grant reimbursement comes in. Local governments live with rigid budget calendars just like Federal and state entities. While it is valid and important to maintain control processes to protect against malfeasance, those controls can be built on the assumption of honesty, rather than the assumption of dishonesty and structured to protect local, as well as Federal, coffers. Second, some of our most effective and vital regional radio systems include governance arrangements wherein participating jurisdictions concede some of their powers to a Joint Powers Authority and obligate themselves to provide a continuing funding stream to the system. This funding takes the form of both annual "per user" fees

and initial and recurring capital contributions. In most cases jurisdictions buy their own end-user equipment in conformance with system standards. The annual fee pays the costs of maintaining, operating, and in some cases replacing, the shared infrastructure. Often, Federal and state agencies are reluctant or restricted by laws and regulations from committing to these on-going funding arrangements. They become a special class of partners whose financial commitment is not as reliable. For interoperability to be effective, all parties must carry their share of the on-going financial load. It is important to note here that, while the recent surge in Federal grant support to communications system is welcome and sorely needed, this type of funding quietly ignores that each piece of equipment we buy now has a finite and largely predictable life. That life is shortened in many instances by the march of technology, wherein the outdated equipment become the limiting factor preventing modernization, and by regulatory change which sets a definite end to the usefulness of some equipment, serviceable or not. Grant funding as we have been doing the last several years does not address the need for long term funding innovation.

While there is an ongoing need for NTIA to remain separate from the FCC, there is also a need for cooperation in the management of some Federal frequencies to improve interoperability. The paradigms in which many Federal agencies operate (need for a high level of security mandating encryption) are much different from the local and state paradigms. As a result, these Federal entities are very reluctant to work with non-Federal first responder organizations on Federal frequencies without the non-Federal users having radio equipment with 'federal grade' encryption – which the Federal entities will not allow to be keyed to Federal systems as a matter of normal policy. First, the blanket imposition of encryption increases costs dramatically. In fact, we all know that most transmissions at the scene of an incident do not require encryption. The adversaries know what they did. They may be lurking in the shadows planning a second strike, but most, if not all, of what they hear on the public safety radio during the crisis will not change those already laid plans. On the other hand, locals need to know on which partners they can depend if the incident comes to their door. SAFECOM is properly positioned to act as the bridge between these two paradigms. The height of the incident is not the time to learn that a partner wants to help but can't because they don't trust you with an electronic key to secure information that doesn't need to be secure. Second, the incident command team needs a communications environment in which they can communicate freely. Therefore they need to know what organizations are partnering with them and which channels are linking which entities. Allowing local participants the use of certain identified Federal channels during crisis can speed the development of cooperation and the sharing of information. Until recently, Federal channels have been divided among agencies with little attention to shared frequencies except as negotiated by the agencies among themselves. That may leave the local incident with a relatively large number of connections to make to Federal partners and turn the local interoperability channel in to a Federal coordination channel. NTIA should continue efforts to develop shared channel plans, including designated non-encrypted channels, for both Federal agency coordination and Federal to local cooperation. The SAFECOM Program provides the forum and increasingly reflects the mid set to advance cooperation in this manner.

And while we discuss Federal spectrum regulatory agencies, the FCC has before it today a series of recommendations to improve interoperability as part of its ongoing 700 MHz proceeding. These recommendations, developed by local and state practitioners as part of a Federal Advisory Committee chartered by the FCC for this

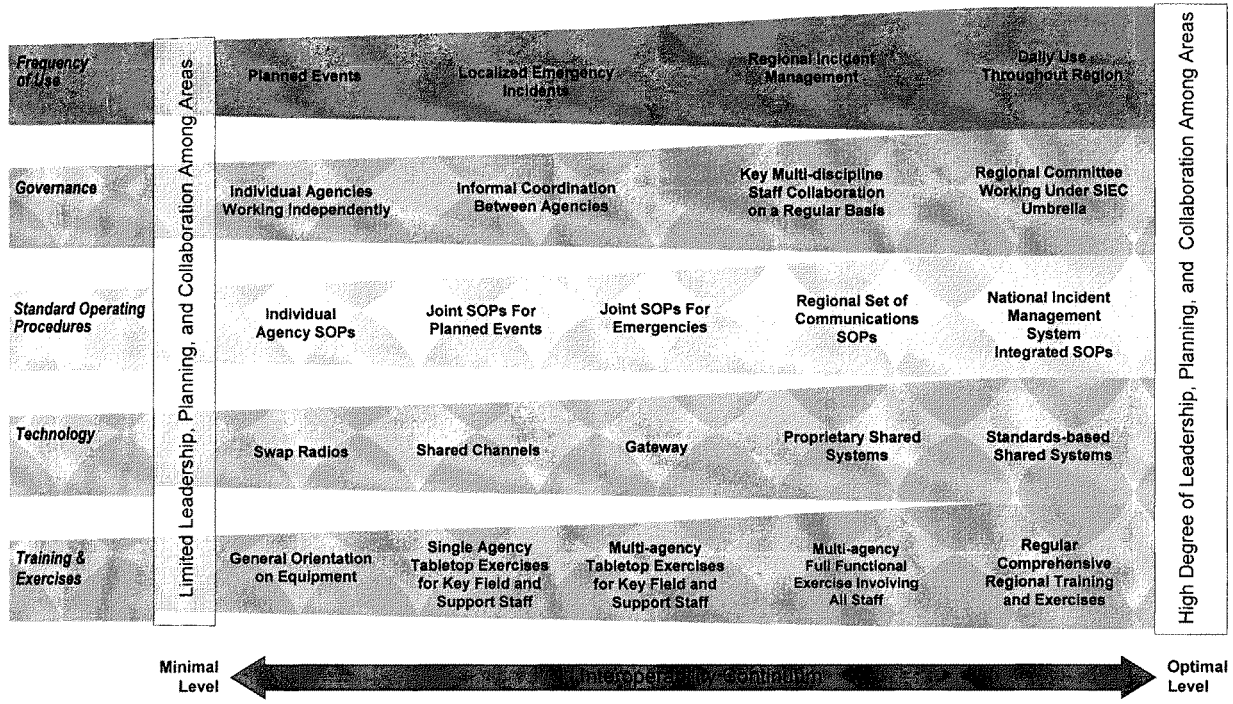
purpose, are essential to the rapid and successful implementation of the "system-of-systems" approach to nationwide interoperability envisioned by SAFECOM. There are times when the FCC must establish some basic requirements of all public safety users in order to ensure interoperability, and these have been succinctly outlined in the final recommendations of this Public Safety National Coordination Committee to the FCC.

Finally I want to spend a minute on the Statewide Interoperability Executive Committee movement. The FCC offered the charter for these committees to operate at the state level, but including local and Federal partners. Their task is to plan for and manage new frequencies that are to become available when television moves out of the 700 MHz spectrum range. California, like several other states has decided to expand the SIEC charter to cover all the families of frequencies that public safety professional share across the state. We are going to consolidate those old system-specific plans I spoke about earlier. We are assembling a cross discipline team, as I described above, including law, fire, emergency medical, and emergency management professionals to rewrite the existing plans, hopefully using some of he language the SAFECOM Program is working on with the two cities. Those conversations will provide a background for a separate committee made up of the California state agencies that are significant users of public safety radio. Their charge is to develop a plan for modernization of state systems to replace obsolete equipment, achieve narrow-banding as soon as possible, and improve interoperability between state agencies and across levels of government.

Thank you again for the opportunity to speak before you. I look forward to our discussion.

SAFECOM

Interoperability Continuum



Mr. PUTNAM. Thank you very much. And again, I apologize for the fact that we're going to have to cut this short.

I'm going to give everyone the opportunity to ask the question of the day before I have to run off to vote, we'll begin with Ms. Lischke, and I would ask all of you to please keep your answers to a minute.

What specifically can the Federal Government do, for the short term, for the State and local governments that you represent, to improve interoperability?

Ms. LISCHKE. Again, I believe the support for the SAFECOM program helps us in the long term. And in the short term, again, we're working with the SAFECOM project and the RAPIDCom project. But it's coming up with some of the patch devices that David Boyd was talking about, that allows us to connect different types of radios together.

And also working with the Department of Defense program that is putting out land mobile radios, which is a commercial off the shelf product and provides us some of the interoperability we need until the long term radio that David Boyd was talking about, the joint tactical radio, comes out.

Mr. PUTNAM. Thank you very much. Mr. Stile.

Mr. STILE. Thank you. I would say that we need to have the SAFECOM continue with their programs at least to better provide more of the training, more of the ability to get information out to the State and locals, local government needs to be funding wise, needs to come down from the State to the local level. I would actually like to see it go to the regional level, but there is no regional point that those moneys could be funded to.

So it needs to come from the States to the individual localities. And I personally believe that it's necessary for SAFECOM to continue their program, as to what they've started out with and what they're doing.

Mr. PUTNAM. Thank you, sir. Chief.

Chief NEUHARD. Thank you, Mr. Chairman. I have three suggestions as to what the Federal Government can do to continue to help us as first responders. First and foremost, we need continued grants that not only include equipment but also include planning, training and exercise money, specifically for interoperability issues.

Second, there is, as you heard today, a real need for continued facilitation and coordination at all levels of Government. I think now SAFECOM is on track and we need to see that continue.

And third, finally, we need a long term commitment to see interoperability through. As you've learned today, it is not a steady State. It is going to require continued funding and continued focus. So at the Federal administrative level, and from Congress, we need money and focus. Thank you.

Mr. PUTNAM. Money and focus. Thank you.

Mr. Worden.

Mr. WORDEN. Yes, sir. First, the support for SAFECOM and the recognition that a single agency developing standards is critical. Second, elimination of duplication and, please don't get me wrong, I don't want to eliminate duplicate source of money, but when those sources of money come with duplicate guidance, it leads us off in too many directions.

Third, cross discipline planning at the Federal level to enable locals to plan more effectively for the Federal partners who will join them during events, rather than having to deal with each agency separately or distinctly different approaches to planning from the different Federal agencies.

Finally, for all the funders to recognize the multi-year nature of the funding that's needed both for planning and for implementation. It is very difficult to plan and fund a well thought out system in the funding cycles we have, and having to make investments in one grant cycle with the fear that they won't be eligible in the next grant cycle has paralyzed some local operations.

Mr. PUTNAM. Thank you very much to all of you. Before we adjourn, I just want to apologize again for the brevity of this, particularly those of you who have traveled. Unfortunately, that's just the way the vote schedule works.

I appreciate your knowledge and experience and thoughts that you and panel one shared with us, as well as the efforts of the subcommittee members and subcommittee staff, particularly Shannon Weinberg and Felipe Colon, as well as Grace Washbourne from the full committee.

We're grateful, terribly grateful for the every day heroes, the first responders in our communities who put themselves in harm's way on our behalf and run into buildings that everyone else is running out of. We look forward to a nation that is safer and better protected through improved communications capacity and interoperability and also looking forward to saving the lives of those men and women who do put themselves in harm's way as a result.

I want to thank everyone who participated in this, and in the event, and this is certainly the case, that there are additional questions that we did not have time for, the record will remain open for 2 weeks for submitted questions and answers. We will be submitting those to you, and we look forward to your response.

Thank you so very much. With that, the subcommittee is adjourned.

[Whereupon, at 3:55 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

Questions from Project SAFECOM:

1. *How can states and local governments best be empowered to become the focal points for making sure that intra- and inter-state regions have interoperable wireless communications capabilities?*

Adoption of a common approach to emergency management such as the California Standardized Emergency Management System described below provides a common frame of reference of emergency responders within which they can define their communications needs and practices, including interoperable communications. However, in order to move from interoperability solutions that add hardware to create ad hoc solutions governments must incorporate interoperable communications in to the architecture of their public safety radio communications systems. Those intermediate –size cities that migrated to trunked radio systems for the entire city, rather than for just police or fire as in the larger cities, found themselves forced to define cross discipline communications needs as they built their talkgroup plans.

The process instituted by the Federal Communications Commission when the new allocations for interoperable channels in the 700 MHz range were announced provided for a Statewide Interoperability Executive Committee (SIEC) [or the FCC-designated Regional Planning Committee (RPC), should the state elect not to assume the responsibility to manage the interoperability spectrum], to manage those channels. The concept is well proven and works well when the SIEC truly consists of members at all levels of government, and is representative of all disciplines within public safety. In large states, it can be extended closer to the local level through the creation of subcommittees within a state operating under the umbrella of the SIEC. Future federal grant programs should emphasize provide funding opportunities for the initial costs of developing SIECs and their first planning products, and require adoption of a plan by that committee as a prerequisite for grant funding of communications equipment consistent with the plan. Further requiring those committees to coordinate their plans with the Regional Planning Committees and adjacent state's SIECs will ensure that communications practices will be standardized across a large enough area to make large-scale mutual aid response practical.

2. *How has your state been able to coordinate its emergency, law enforcement, and public health and safety communities to ensure that first responders can communicate? How do you overcome "turf issues" – that is, knowing who is in charge in a given event and ensuring that all responders are working together in the most effective and efficient manner?*

Following the disastrous Oakland Hills Fire of October 1991, the state legislature passed and the Governor signed Senate Bill 1841, which became California Government Code §8607. This required the development by regulation (California Code of Regulations (CCR) §2600 et seq.) the Standardized Emergency Management System (SEMS), which was completed and implemented statewide on December 1, 1996.

This system was based on some long established principles such as:

- The Incident Command System
- Multi/inter-agency Coordination
- Mutual Aid
- Operational Areas

The system recognized five organizational levels of emergency response:

1. Field – where the Incident Command System is used and most emergencies develop;
2. Local – As in local government, cities, counties and special districts
3. Operational Area – Consisting of a county and all the cities and subdivisions within, activated for coordination of information and resources;
4. Region – As in California's Mutual Aid regions, consisting of multiple Operational Areas geographically related
5. State – As in the State Emergency Operations Center in Sacramento

Five Functions:

1. Management – providing the overall direction and setting priorities for an emergency;
2. Operations – Implements priorities established by management (usually functions such as Law Enforcement, Fire & Rescue, Medical & Health, Care & Shelter, etc.);
3. Planning/Intelligence – Gathers and assesses information;
4. Logistics – Obtains the resources to support operations, Communications management is a responsibility of the Logistics Function;
5. Finance/Administration – tracks all costs related to the operations.

In addition, all state agencies are required to use SEMS when responding to a multi-agency or multi-jurisdictional emergency. All local jurisdictions are required to use SEMS in multi-agency or multi-jurisdictional emergencies to be eligible for state reimbursement of 75% of the local share of response-related personnel costs in federally declared disasters.

SEMS compliance is enhanced through the development of an Approved Course of Instruction (ACI) (Government Code §8607 (c)). Also, there is a requirement for After Action Reports (AAR) and a SEMS Maintenance System (CCR §2600) to address changes and improvements in the system.

Compliance with SEMS places the responsibility to direct communications systems supporting the incident at the Field level in the control of the Incident Commander. While Fire agencies are more likely to maintain trained staff for the five Incident Command functions and more readily transition to ICS, other agencies maintain some or all of the skills. Sometimes an ICS team from the California Department of Forestry ad Fire Protection will provide the ICS staff under the direction of a local or state official from another discipline.

3. *How helpful have the federal grants been in helping your state and local governments do what it needs to do to make its communications systems interoperable? Do state and local governments need federal grant programs that are exclusively for the purpose of acquiring new or upgrading existing communications equipment or do they prefer grants that can be used for more broadly defined homeland security activities that include improvements to communications systems?*

Grants to date have been effective in procuring the hardware needed to achieve interim interoperability. They have only begun to become effective tools in the planning, training, and governance areas of developing interoperability which are often much more difficult to resolve. Targeting grants to specific subject areas or classes of equipment is NOT a sound idea. Jurisdictions vary widely in the approaches to interoperability, both interim and long term, that will be most effective. Including as a prerequisite for equipment funding the adoption of plans

for the management of events, communications during events, and the maintenance of systems and protocols for cooperation between events, coupled with the funding and technical assistance in preparing those plans may be an effective tool. Grant guidance should focus on desired outcomes (effective management of responses to emergencies) and leave the selection of methods to those who will be doing the responding.

4. *You spoke in detail about the current federal grant-funding structure. What specific recommendations do you have for improvement in administering the homeland security grants relating to interoperable communications systems?*

Grant guidance wording should remain relatively constant from year to year in order to reduce the burden on states as grants managers and localities as applicants in tailoring applications.

Grant programs should offer some mechanism to spread across several years the integrated costs of analysis, planning, engineering, procurement, implementation, and training for complex systems. Localities have been encouraged to procure the equipment first when funds are offered in part because they fear that if the spend the money on the necessary preliminary steps the grant program will change and they will never get to buy the equipment for which they prepared.

Planning prerequisites for the procurement of equipment are a sound idea but have not been well implemented. Jurisdictions need access to guidance in developing plans, information exchanges about successful planning elsewhere, and a point of review or acceptance of their plan.

5. *GAO and the FCC have recognized the important role of the state in public safety interoperability planning. However, states are not required to establish statewide management structures or to develop interoperability plans. In addition, no requirement exists that interoperability of federal communications systems must be coordinated with state and local government communications systems. Are state interoperability committees or offices necessary? If so, why? If your answer is "yes," what do you think should be the makeup of a state interoperability management office?*

Statewide Interoperability Management offices are critical to the success of the effort. They can and should perform the following functions:

- Provide executive support and funding for the SIEC and publish its work product as parts of the State Emergency plan and Mutual Aid Plans
- Serve as reviewing agency for local and regional plans to ensure conformance with the statewide plan
- Serve as a frequency management clearing house assisting local, regional, and state agencies in developing frequency implementation plans the make maximum practical use of the spectrum given the terrain and other factors that affect the use of the same channel in different areas.
- Maintain an information sharing system to provide local and state agencies easy access to best practices and lessons learned

This organization need not be large. One or two communications professionals assisted by two or three analysts should be able to perform this function in a large state provide they have a

sufficient budget to assist local and state participants to travel to SIEC and other meetings and to hire consultants when needed. More staff may be needed if the office also acts as the FCC license holder for the state.

Committee: House Government Reform, Subcommittee on Technology, Information, Policy, Intergovernmental Relations and the Census
Hearing Date: September 08, 2004
Hearing: National Guard/Reserve
Member: Representative Adam H. Putnam
Witness: Mrs Maureen T. Lischke
Question: #1

First Responder Interoperability

Question. Please describe, in your experience, how interoperability has improved since 9/11. What concrete steps have we, as a nation, taken to improve first-responder interoperability?

Answer. The major improvement has been the recognition by all stakeholders of the importance of public safety response through more effective and efficient interoperable wireless communications. There are many groups at the federal, state, and local level addressing the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks. A very important step was taken with the establishment of SAFECOM[1] under Department of Homeland Security. SAFECOM is providing the leadership to address interoperability, and the National Guard supports and is cooperating with that effort.

The National Guard Bureau's strategic approach to meeting IT requirements to support the homeland security mission is the Joint CONUS Communication Support Environment, and it includes partnership with the Department of Homeland Security's SAFECOM program to achieve interoperability.

It is expected that the National Guard will be the first military responders to a homeland security incident. The National Guard with its connectivity to federal IT networks and state networks has enormous potential to assist in addressing the national challenge of interoperability. Taking advantage of the dual (state and federal) role of the National Guard, the National Guard Bureau has developed an IT strategy that could assist in attaining or improving interoperability for the homeland security mission within the states. That strategy is embodied in an IT initiative labeled "Joint CONUS Communication Support Environment (JCCSE"). This initiative is addressed in more detail in the answer to question 5.

The National Guard Weapons of Mass Destruction Civil Support Team's (WMD CST) Unified Command Suite (UCS) is the most prominent component of the National Guard's current IT capabilities that is tailored directly for support of first responders for the war on terrorism. The UCS provides the National Guard WMD CSTs with the capability to communicate with the incident commander and emergency response personnel at an incident site, and provides satellite communications that support "reach-back" to vital databases and staff that support the deployed

---

[1] *Wireless Public SAFEty Interoperable COMmunications (SAFECOM) program under auspices of the Department of Homeland Security. It is an umbrella program that encompasses various public safety wireless initiatives and involves wide-ranging activities.*

WMD CSTs. The National Guard requires IT capabilities that extend from theWMD-CSTs at the incident site to local levels to state entities and finally to the federal level. The GuardNet, Air National Guard Enterprise Network, and Warrior Net provide backbone network and satellite broadcast capabilities that extend information exchange capabilities to armories and Air National Guard bases and distance learning training facilities/command and control sites throughout the Nation. Additionally, many of the states/Territories have developed robust intra-state network capabilities that can further extend the communications reach.

The National Guard State Standing Joint Force Headquarters have access to the state's limited deployable communications capabilities—such as HF/UHF/VHF radios. In some states, such as California, there are more robust capabilities available to enhance interoperability at the incident site. Immediately after the Sep 11th 2001 attacks, the National Guard Bureau began to look at the requirements, and specifically how it can leverage and enhance these capabilities to support the new threat environment. These new concepts were employed in support of recent National Special Security Events (NSSEs) such as the G8 Summit and the funeral of former President Reagan.

Experience to date in these real-world events and exercise scenarios has demonstrated to the National Guard Bureau leadership the importance of improving the capabilities to facilitate inter-state collaboration and to provide more robust interoperable communications capabilities at an incident site. To meet these needs, the National Guard Bureau is collaborating with NORTHCOM on a proposal to task the National Guard to provide a Joint CONUS Communications Support Environment (JCCSE) that will extend information sharing capabilities from the national- to state/local-levels, and to the incident site.

Committee: House Government Reform, Subcommittee on Technology, Information, Policy, Intergovernmental Relations and the Census
Hearing Date: September 08, 2004
Hearing: National Guard/Reserve
Member: Representative Adam H. Putnam
Witness: Mrs Maureen T. Lischke
Question: #2

First Responder Interoperability

Question. Please describe the current capability for the National Guard to provide military assistance to civilian authorities (MACA) in terms of enhanced communications interoperability, including a description of the use and capabilities of the Civil Support Team Communications vehicles.

Answer. Each of the 32 National Guard Civil Support Teams (CST) has been equipped with a Unified Command Suite (UCS) that provides the primary means of communications. The UCS is a highly mobile, fielded communications system. It is a non-developmental item, a variant and reconfiguration of the Joint Base Station. The UCS operates in both urban and undeveloped areas, utilizing portable and fixed equipment. The UCS provides real-time voice, data, and video access (unclassified through Top Secret) among the following information elements: CST members, local and state emergency response agencies, lead federal agencies and supporting military activities. The UCS consists of a combination of standard commercial-off-the-shelf (COTS), non-developmental item (NDI), and existing military equipment to provide the full range of communications necessary to support the CST mission and consists of the following subsystems:

- A commercial truck to carry the communications-electronics suite. The truck is equipped with an on-board power generation and distribution system and two operator positions in the rear of the vehicle. The UCS is air-transportable on a C-130 or larger military transport aircraft.
- Radio Frequency (RF) Communications Subsystem that includes sufficient tactical voice equipment to ensure a dedicated line of sight (LOS) voice circuit for exclusive use of the CST survey teams. Additional voice circuits are provided for fire, local law enforcement and emergency service interoperability.
- VHF Line of Sight (LOS) voice net, with a base station radio, repeater system and hand-held radios which are compatible with the base station.
- UHF Line of Sight (LOS) voice net, with three base station radios, hand-held radios, and additional adapters and antennas.
- Telephone subsystem to include: Cellular phone (non-secure), one INMARSAT terminal that provides wide-area telephone connectivity and secure phone, STE, as well desktop terminals to support tactical planning and reporting, and two (2) IRIDIUM secure satellite handsets.
- Automatic Data Processing (ADP) subsystem to include LAN/ WAN connectivity to military and commercial systems providing both secure and non secure operation, all fully interoperable with standard DoD and federal architectures and protocols to include SIPRNET and NIPRNET.

- Ancillary equipment subsystem includes antennas and RF patch and feed through panels that provide connections for patching both mobile and fixed antennas to their associated transceivers.
- Power generation subsystem providing uninterrupted electrical power for on board circuit architecture and environmental control units, to include a 15 kilowatt-on-board diesel generator and back-up battery system.

As the primary means of communication supporting the CST, the UCS acts as a hub to provide a common operational picture (COP) for planning and executing an incident response. It serves as the node that controls communications with the CST survey teams at the incident site and passes critical, time-sensitive, information between the CST and Incident Command Post. The UCS also provides "reach-back" communications for connectivity with higher authority and technical support agencies, such as the Defense Threat Reduction Agency (DTRA). Its critical role in the C4I architecture of consequence management requires the UCS to deploy with CSTs, communicate while en-route to an incident, and once on scene, provide a robust communications capability. The design of the UCS provides flexibility in establishing communications with many agencies and activities and it is capable of utilizing all necessary frequency bands to ensure adequate voice and data connectivity. Wideband communications and a robust cellular and landline telephone system permit rapid and complete transfer of large data files to support mission planning and reporting. A family of handheld radios and base stations incorporated into the UCS ensures radio connectivity with local emergency service units.

Committee: House Government Reform, Subcommittee on Technology, Information, Policy, Intergovernmental Relations and the Census
Hearing Date: September 08, 2004
Hearing: National Guard/Reserve
Member: Representative Adam H. Putnam
Witness: Mrs Maureen T. Lischke
Question: #3

First Responder Interoperability

Question. Please describe, if not prohibited, some of the domestic counter terrorism exercises in which the National Guard has participated with local first responders.

Answer. The National Guard has been an active participant with government agencies, state authorities, and local first responders in a number of large exercises. As an example, the National Guard WMD CSTs participated in the following exercises (listed by FEMA region):

FEMA Region I: The 1st CST of the Massachusetts National Guard conducted a "Dirty Bomb" training exercise on 16 May 2004 with the City of Boston Fire Department and Emergency Medical Service, Massachusetts State Police, Department of Justice, Division of Alcohol Tobacco and Firearms (ATF), and the Federal Bureau of Investigation (FBI) Boston Division.

FEMA Region II: The 2nd CST of the New York National Guard conducted a training exercise from 26 Aug – 3 Sep 2004 with New York City First Responders, New York State Police and the New York National Guard CBNRE Enhanced Response Force Package (NG CERF-P).

FEMA Region III: The 3rd CST of the Pennsylvania National Guard conducted two training exercises from 5 – 8 April 2004 with First Responders, Emergency Operations Center, Fire Department and State Hazardous Material Team

FEMA Region IV: The 43rd CST of the South Carolina National Guard conducted a training exercise from 21 -25 June 2004 with local First Responders in Florence, SC.

FEMA Region V: The 52nd CST of the Ohio National Guard conducted a training exercise from 16-19 July 2004 with First Responders from the Miami Valley area and City of Dayton.

FEMA Region VI: The 63rd CST of the Oklahoma National Guard conducted a training exercise on 17 April 2004 with the First Responders from the City of Atoka, OK and Oklahoma Emergency Management Agency that incorporated a chemicals and high yield explosive scenario.

FEMA Region VII: The 73rd CST of the Kansas National Guard conducted a training exercise from 3-5 February 2004 with the Kansas University Medical Staff that incorporated decontamination operations.

FEMA Region VIII: The 8th CST of the Colorado National Guard conducted a training exercise

from 17-19 Sep 2004 with the first responders to include Montrose Fire, Eagle River Fire, Durango Fire, Glenwood Fire, Grand Junction Fire, Farmington Fire, Montrose OEM, Mesa OEM, Delta County OEM, Summit County OEM, Gunnison HM, Eagle Hazmat, CSP, Mesa PH, Ouray LEPC, San Juan Basin HD, US DOE, and EPA that dealt with a chemical spill.

FEMA Region IX: The 9th CST of the California National Guard conducted a training exercise from 21-25 June 2004 with the first responders of the City of Las Alamitos, Orange County Fire Department and State Hazardous Material Teams encompassing a "dirty bomb" and radiological scenario.

FEMA Region X: The 10th CST of the Washington National Guard conducted a training exercise on 1 September 2004 with First Responders from around Fort Lewis, WA vicinity and Fort Lewis Provost Marshall.

The following are some of the DoD domestic counter terrorism exercises in which the National Guard has/will participate with local first responders:

The Automated Exercise and Assessment System (AEAS) is a CD-ROM based system that was developed by the National Guard Bureau and SAIC. It is designed to exercise emergency response procedures at the jurisdiction level. It is specific to WMD terrorist attacks on the US. AEAS supports common terminology, standardized ascendancy, integrated communications, unified command structure, consolidated action plans, designated incident facilities (command post, staging area, etc.), manageable span-of-control, and comprehensive resource management based on the Incident Command System (ICS) and supplemented by mutual aid compacts and protocols that accommodate regional and state-level participation. It is being distributed to emergency responders throughout the country with the National Guard Bureau providing exercise facilitation and participation.

Ardent Sentry (AS) is the CDR NORAD-USNORTHCOM (N-NC) approved annual exercise that replaces the Unified Defense (UD) and Amalgam Virgo (AV) exercises. AS 05 is scheduled for six days in April 2005 and will be linked with the Department of Homeland Security (DHS) exercise, Top Official (TOPOFF) 03. Future AS exercises will be N-NC led in even years and DHS led (linked to TOPOFF) in odd years. The focus of AS exercises will be Military Assistance to Civil Authorities and asymmetric threats. Additionally, N-NC has established Vigilant Guard (VG) as a second tier National Guard (NG) exercise attached to the Ardent Sentry series. VG is essentially a series of training and exercising events focused on the enhanced preparedness of the National Guard during periods of heightened threats.

Northern Edge (NE) is a congressionally funded exercise that is conducted in Alaska. Principle training audiences include NG, and all Alaska state agencies. Beginning in FY 05, and in subsequent odd years, N-NC will sponsor the exercise, which will focus on Homeland Defense and Incident Management events. In even years, USPACOM will have scenario lead.

Vigilant Shield (VS) is the N-NC approved annual exercise that replaces the Determined Promise (DP) and Vigilant Overview (VO) exercises. The VS series will be scheduled in Nov of each year. This exercise will focus on strategic war and the homeland defense missions.

Determined Promise 04 had several WMD vignettes in which CA and VA NG participated. Additionally, 40 additional states and territories participated in the simultaneously conducted exercise Guard Magic 04 which utilized the same vignettes and additional injects.

The Amalgam Chief series are CDRNORAD mandated exercises, which were initiated as a result of 9/11 to train staffs, develop and test Operation Noble Eagle procedures, exercise interagency coordination and maintain proficiency at all levels to respond to airborne terrorist threats to North America. These exercises use live-fly targets or simulated aircraft to exercise organizational coordination, and validate C3 among NORAD regions, HQ NORAD, Cheyenne Mountain Operation Center, National Military Command Center, Secretary of Defense and the President.

In addition to these exercises, the National Guard has recently played a key role in three "real world" National Special Security Events (NSSE), the G8 Summit, the Democratic National Convention, and the Republication National Convention. For these three events, the President and respective Governors invoked the authorities provided by Congress' recent legislation, H.R.1588, National Defense Authorization Act for Fiscal Year 2004 section 516, "National Guard Officers on Active Duty in Command of National Guard Units" that changed title 32, section 325 to allow the "dual-hatting" of the National Guard commander under the command of the governor and the President. This new authority has proven to be a key improvement in integrating the federal and state military support to first responders.

Committee: House Government Reform, Subcommittee on Technology, Information, Policy, Intergovernmental Relations and the Census
Hearing Date: September 08, 2004
Hearing: National Guard/Reserve
Member: Representative Adam H. Putnam
Witness: Mrs Maureen T. Lischke
Question: #4

First Responder Interoperability

Question. What steps is the National Guard taking in conjunction with DHS to ensure that National Guard communications capabilities will work with what DHS is supporting at the state and local level? Should there be procurement standards that will encourage interoperability between National Guard and DHS supported systems.

Answer. The National Guard Bureau is working with both the office of the Assistant Secretary of Defense for Homeland Defense and the staff at the Department of Homeland Security with the express goal to synchronize efforts and establish the framework for a strong and ongoing partnership. The National Guard Bureau expects that the National Guard will be the first military responders in nearly every conceivable homeland security instance, and therefore interoperability with civilian emergency management and the first responder community is absolutely essential to the capability to support the National Guard state mission. It is conceivable that under some circumstances the National Guard's IT resources could be used to support or supplement the capabilities of the civilian response sector. Toward these ends, the National Guard Bureau is enthusiastic about the opportunity to participate as an IT partner in the Department of Homeland Security's SAFECOM program and to ensure that whatever capabilities that are developed, are interoperable with other communication used at the state and local level.

Additionally, the National Guard Bureau is working closely with the office of the Assistant Secretary of Defense for Homeland Defense and the Department of Homeland Security on the RapidCom 9/30 initiative that seeks to enhance interoperability capabilities in 10 high threat cities to ensure preparedness in case of a near-term terrorist attack. The National Guard Bureau has identified a state-level National Guard point of contact for each city team, and has provided its distance learning classrooms and video teleconferencing capabilities for RapidCom 9/30 project coordination. Additionally, these distance learning facilities are being made available (if requested) to the Department of Homeland Security to conduct training.

The National Guard believes there should be standards for the public safety interoperable communications within the incident area. There are potential benefits to establishing technical standards that will provide a sound basis for decision-making on procurement actions that move all stakeholders toward the goal of interoperability. Obviously, there are challenges with achieving interoperability-based procurement standards across federal agencies and the degree of difficulty is magnified when state and local entities are included. This challenge clearly speaks to the need for strong leadership on these complex issues through a national-level program like SAFECOM. SAFECOM was endorsed by the Defense Science Board's (DSB) 2003 Summer

Study Report, DoD Roles and Missions in Homeland Security, Nov 2003. That report recommended, "NORTHCOM and the National Guard should proactively support Department of Homeland Security in establishing effective operability standards and in deploying critical communications assets, such as SAFECOM, and also underscores the vital importance of a strong and collaborative DoD (Assistant Secretary of Defense/Homeland Defense and National Guard) partnership with Department of Homeland Security. The National Guard supports the SAFECOM approach.

Committee: House Government Reform, Subcommittee on Technology, Information, Policy, Intergovernmental Relations and the Census
Hearing Date: September 08, 2004
Hearing: National Guard/Reserve
Member: Representative Adam H. Putnam
Witness: Mrs Maureen T. Lischke
Question: #5

First Responder Interoperability

Question. General Blum has said that the Joint .CONUS Communications Support Environment (JCCSE) would make it possible to link every state house to the White House and every police and fire station to the Pentagon, how close are you to doing that?

Answer. The JCCSE is a National Guard term used to describe a general assortment of enhancements to the existing National Guard IT environment that will provide trusted information sharing among federal, state, and local activities. The National Guard's existing IT enterprise connects over 3500 locations in 54 states, territories, and the District of Columbia. LTG Blum recognizes the potential benefits to be derived for Homeland Security and Homeland Defense from enhancing the capability of the National Guard's IT networks, and therefore has repeatedly endorsed the JCCSE as the National Guard's number one IT initiative. The National Guard currently is working diligently with the office of the Assistant Secretary of Defense for Homeland Defense, USNORTHCOM, and the Joint Staff for the implementation of JCCSE, as well as the long-term sustainability of JCCSE capabilities.

Until the full features of the JCCSE are realized, the National Guard Bureau is moving ahead with the development of some of the JCCSE capabilities so that it is prepared should another terrorist event occur. Therefore, this year the National Guard Bureau is improving the National Guard IT network capabilities (GuardNet) to provide enhanced capability as well as reliability, and have already provided enhanced secure communications capabilities (SIPRNET) to all of the Joint Force Headquarters. Additionally, based upon some comprehensive studies, the National Guard Bureau took aggressive action to stand up an enhanced National Guard Bureau Joint Operations Center to provide a focal point to support USNORTHCOM and USPACOM interface to, and collaboration with, the Joint Force Headquarters in all 54 states and territories. At present, the National Guard Bureau is in the process of fielding the Interim SATCOM Incident Site Command Sets (ISISCS) in 12 states. ISISCS will provide interoperable communications capabilities at an incident site, as well as reach back satellite communications capabilities from the incident site to the State Standing Joint Force Headquarters and beyond. In short, the National Guard Bureau has already aggressively begun the process of achieving LTG Blum's stated goal of achieving nationwide information exchange capabilities from the incident site—to the state-level—and to the national-level. There is much more to do to meet the goals of the JCCSE initiative. The National Guard Bureau feels that the JCCSE is the right direction to provide a robust infrastructure that leverages current capabilities to the maximum extent possible, and substantively enhances the National Guard's capabilities to respond to the entire spectrum of potential operational missions—from natural disasters to terrorist attacks.

U.S. House of Representatives: Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
"Project SAFECOM: More Time. More Money. More Communication? What Progress Have We Made In Achieving Interoperable Communication Between Local, State, and Federal First Responders?" – September 8, 2004

Responses to Questions for Mr. John Muleta
Federal Communications Commission
October 22, 2004

Question 1: What steps can the FCC take immediately to ensure that first responders use a common set of terms and radio protocols when responding to emergencies?

Response: The Public Safety National Coordination Committee (NCC) recommended a specific list of channel names to be used by all public safety licensees. The NCC was a Commission-created Federal Advisory Committee. The Commission is considering the NCC's recommendation in the context of a rule making proceeding that addresses public safety issues. Given the ongoing nature of this rule making, I am unable to further discuss the merits of the NCC recommendation at this time, but I would be pleased to provide additional information upon the conclusion of the proceeding. We anticipate the decision will be released before the end of the year.

I should note, however, that when the Commission previously considered the channel nomenclature issue, it expressed concern about the practical and administrative burdens that could flow from such a requirement. We continue to believe that the common nomenclature issue must be evaluated in the context of the over 40,000 public safety licensees, each of which has its own organizational culture and operational requirements. In addressing the nomenclature issue, we are mindful that actions we may take could affect the administrative procedures, budgets, logistics and training requirements of thousands of public safety entities. In the interim, we will continue to work with the public safety community regarding initiatives designed to promote effective public safety communications, particularly during emergencies.

Question 2: How does the FCC view the recommendations in the Department of Commerce's recent report entitled *Spectrum Policy For the 21st Century – The President's Spectrum Policy Initiative: Report 2, Recommendations From State and Local Governments And Private Sector Responders?* Specifically, the Commerce report recommends establishing a Spectrum Management Advisory Committee, led by DOC, with participation of FCC and DHS. This Spectrum Advisory Committee would, among other things, work to reduce the time required to coordinate new spectrum uses and perform analysis of potential interference issues, suggesting ways to make spectrum use more efficient and effective.

Response: First, I would like to commend the efforts of Secretary Evans, NTIA Administrator Michael Gallagher and their staffs in spearheading the *President's*

Spectrum Policy Initiative Report (Report) initiative released in June, 2004. The Report captures some of the most important spectrum issues facing the country today. We are pleased that many existing Commission spectrum policies and proposals are congruent with those discussed in the Report. For instance, the Commission's Secondary Market rules allow for the benefits of spectrum leasing and other tools that hold promise for significantly more efficient use of wireless spectrum. Also, the Commission has worked with the Administration to provide technical assistance related to legislation for extended auction authority and the authority to impose spectrum fees, as recommended by the FCC's Spectrum Policy Task Force. These initiatives fit squarely in the Report's goal to "Establish Economic and Efficiency Incentives."

The FCC's Wireless Telecommunications Bureau (Bureau) spectrum "audits" are another example of how past and ongoing FCC initiatives advance certain recommendations in the Report, *e.g.* the directive to "Identify and Address Unsatisfied Spectrum Requirements for Public Safety." The Bureau has conducted detailed surveys of spectrum use to identify currently unused spectrum. Also, in the Commission's recent Report and Order in the 800 MHz public safety interference proceeding, the Commission achieved the dual goals of addressing unacceptable interference to 800 MHz public safety systems and, at the same time, identifying an average of 4.5 MHz of additional spectrum that will be made available for public safety applications.

The Report directs the National Telecommunications and Information Administration (NTIA) to establish a Spectrum Management Advisory Committee (Committee) that would reside in the Department of Commerce. The Committee would be comprised of various stakeholders, including representatives from state, regional and local sectors, industry, academia and consumer groups. The Report also invites and encourages the Commission to participate in this forum as appropriate. To the extent that such a spectrum advisory committee, or similar entity directed to efficient spectrum use is formed and funded, we will provide expertise and assistance as necessary to help realize this worthwhile goal. Our participation in that regard would represent an extension of our long-standing cooperative ventures with NTIA and our close association with the Department of Homeland Security, on public safety communication matters.

Interoperability: A Local Perspective

Testimony by Chief Michael P. Neuhard
Fairfax County Fire and Rescue Department
before the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Wednesday, September 8, 2004

Questions and Answers
October 13, 2004

1. **How can state and local governments best be empowered to become the focal points for making sure that intra and inter-state regions have interoperable wireless communications capabilities?**

   Developing public safety communications interoperability must always be a locally, practitioner driven process. This bottom-up approach is the only way to ensure that local, regional, state, and federal public safety agencies can adequately partner to create truly multi-jurisdictional and multi-disciplinary communications interoperability.

   Empowering local and state governments to follow this bottom-up model is a responsibility that the Department of Homeland Security's SAFECOM Program recently undertook. Through the creation of the first ever consensus grant guidance, SAFECOM --- in partnership with local and state public safety and government associations --- has successfully mapped out some necessary requirements for public safety wireless communication technology grants. This guidance has been used by the Federal Emergency Management Agency and the Office of Community Oriented Policing Services, and will hopefully be used in all future Office of Domestic Preparedness communication grants.

   The Commonwealth of Virginia used this grant guidance and bottom up approach to create a statewide strategic plan for public safety communications. Virginia's planning process emphasized local and state practitioner involvement and leadership every step of the way, including local leadership of the interoperability governance structures to oversee the state's continued efforts.

   It has been critical for Virginia to have SAFECOM as a single access point in the federal government to provide guidance, resources, and assistance in our process. Equally as critical is the continued consolidation and coordination of all federal programs that support communications interoperability at local and state levels, including programs offering grants, technical assistance, and other types of resources.

2. **How has your state been able to coordinate its emergency, law enforcement, and public health and safety communities to ensure that first responders can communicate? How do you overcome "turf issues" - that is, knowing who is in charge in a given event and ensuring that all responders are working together in the most effective and efficient manner?**

With the support of the Department of Homeland Security's SAFECOM Program, the Commonwealth of Virginia recently completed the first step in an effort to enhance interoperability through the development of a strategic plan for improving statewide interoperable communications based on this locally driven approach. Virginia's strategic planning process was driven from the local level up and focused on building support for the plan at every level of government.

According to Chris Essid, the Virginia Commonwealth Interoperability Coordinator (CIC), "The focus placed on ensuring that local first responders drive the process when creating interoperable communications plans has been long overdue. Who better to identify what works and what does not work than the very same public safety responders that use radios on a daily basis to save lives?"

Charles Werner, deputy fire chief for the city of Charlottesville was recently selected to serve as the Virginia Interoperability Executive Committee Chair, which validates the practitioner driven governance model as outlined by SAFECOM. According to Chief Werner, "Local first responders across Virginia have been actively involved in the Strategic Plan development through focus groups and planning processes. The Commonwealth of Virginia has demonstrated this philosophy through action – a very powerful demonstration of trust."

The Virginia planning process can serve as a model to other jurisdictions developing strategic plans for interoperable communications. SAFECOM developed and will soon offer the Statewide Communications Interoperability Planning (SCIP) Methodology as an effective model that other states may adapt to their particular needs.

National Incident Management System (NIMS) is an essential element of achieving interoperable communications and provides some guidance as to how to work during a multi-agency event. In Virginia, the Virginia Department of Fire Programs and Virginia Department of Emergency Management have been working collectively to deliver NIMS instruction throughout the state.

3. **How helpful have the federal grants been in helping your state and local governments do what it needs to make its communication systems interoperable? Do state and local governments need federal grant programs that are exclusively for the purpose of acquiring new or upgrading existing communications equipment or do they prefer grants that can be used for more broadly defined homeland security activities that include improvements to communications systems?**

Virginia has been fortunate in receiving some of the designated communications grant funding for the purchase of equipment. However, although these funds are helpful in equipment procurement, they are limited in scope such that grantees cannot use the funding for the necessary planning, maintenance, training, or assistance required to effectively implement any communications system. These other aspects of implementing wireless communication systems are not adequately funded by federal grant programs. And where available, those federal resources for technical assistance are not coordinated with other efforts across the government. The result is diverse and often conflicting direction to local and state agencies. This point again emphasizes the need for continual adoption of coordinated grant guidance for planning, building, upgrading, maintaining, and training on public safety communication systems.

Broader homeland security grants also lack the necessary communications - specific resources to allow for adequate development or implementation of communication systems at the local or state level. Communications is just one of many important needs within broader state strategies, and frequently loses out in the prioritization process to other preparedness efforts. Continued specification of communications funding is necessary to ensure a forward path to interoperable communications across the nation. This includes technical support to which local and state governments can turn for assistance. Often these systems are very complex and accompanying consultation is expensive.

4. **Much attention has been focused on the grant-funding structure. What specific recommendations do you have for improvement in administering the homeland security grants relating to interoperable communications systems?**

Coordination is the key. The current structure for homeland security and justice related grants is fragmented due to diverse and overlapping authorities. This situation causes confusion at the local and state level when dealing with requirements for public safety communication and interoperability. Future grants for communications efforts should be aligned with the existing grant guidance; should provide funds for planning, maintenance, and training; and should be designated as communications specific rather than rolled under broader homeland security programs.

Grant applications must be simplified at the state and local level. While there are many online applications that are very effective such as the Fire Act Grant and other ODP online applications, when many of the grants go through the states to localities, the whole process reverts back to a paper grant process, which is tedious and overwhelming. Something must be done to provide an online process, which conforms to what has been achieved at the federal level. This online application process evens the playing field for all grant applicants and it provides error checking within the process. Again, all of this must follow consistent grant guidance across all federal grant programs. SAFECOM is the right place to provide this grant guidance.

Time schedules and deadlines must be realistic. Too often time frames have been too short to do what is necessary. The mandated time deadlines must include the necessary time to plan, design systems, negotiate contracts, and implement these systems. This becomes even more critical when systems are crossing over disciplines, agencies, and/or jurisdictions. Ideally grants should promote regionalized approaches for interoperable communications.

5. **GAO and the FCC have recognized the important role of the state in public safety interoperability planning. However, states are not required to establish statewide management structures or to develop interoperability plans. In addition, no requirement exists that interoperability of federal communications systems must be coordinated with state and local government communications systems. Are state interoperability committees or officers necessary? If so, why? If your answer is yes, what do you think should be the makeup of a state interoperability management office?**

State interoperability committees are emerging across the country. More importantly is how these committees are governed – practitioner driven is a must. Given the considerations of 700 MHz, 800 MHz and interoperability in general, the only way to ensure awareness and coordination is through a process that links at the local, state, and federal levels. The Virginia methodology involved local practitioners across the state. This identified a number of initiatives that were underway and opened some doors of opportunity for neighboring localities to consider joint ventures.

The statewide interoperability planning process undertaken by the Commonwealth of Virginia is a very good case study of a methodology that works. The key factor in its success to date is that it is driven by local first response agencies. Mandating states to establish interoperability committees or officers might not be the best way to achieve what is really necessary – cooperation among and between local and state agencies. Local elected and appointed officials have to come to believe that it is in the best interests of

their citizens and taxpayers that they engage in a cooperative effort with other jurisdictions and the state on wireless radio interoperability issues for emergency response to all hazards. For the federal government to encourage that cooperation could be very beneficial. This could be done by posting (at SAFECOM) success stories about states that have them and providing some federal funding for statewide interoperability planning processes.

There are a number of key components required to achieve a comprehensive interoperability strategy. These elements help to analyze a particular plan and determine what areas are yet to be addressed. This changes in each area, depending on what has already been done, funding levels, available, etc. This was identified through SAFECOM's Rapidcomm Project. Through that process, the SAFECOM Interoperability Continuum was developed which provides planners an overview of the various interoperability components and a way to better understand where their interoperability plans may be improved.

QFR from Congressman Putnam

House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census

September 8, 2004, Hearing

The following question was submitted for SAFECOM response:

GAO found that the current federal grant structure does not fully support statewide planning. In addition, uncoordinated federal and state level grant reviews limit the government's ability to ensure that federal funds are used to effectively support improved regional and statewide communications systems. Can you please describe DHS' efforts to address GAO's findings?

ANSWER: The Department of Homeland Security (DHS) firmly believes that for any statewide proposal to succeed, the statewide plan will have to be developed from the bottom up. Over 90% of the nation's public safety communications infrastructure is owned by localities and states - a fact that highlights the need for practitioner-driven solutions. This principle is observed in relevant initiatives and programs administered by DHS.

SAFECOM recognizes that statewide bodies are a critical mechanism for coordinating public safety communications and interoperability efforts. Statewide planning bodies play a vital coordination role by receiving important input from public safety practitioners, and SAFECOM will encourage the development of appropriate statewide bodies through its Fiscal Year (FY) 2005 grant guidance. DHS, through the SAFECOM Program, has created coordinated grant guidance that outlines eligibility for public safety communications grants, the purposes for which grants may be used, and guidelines for implementing a wireless communication system. The SAFECOM grant guidance was included as part of the Department of Justice's Office of Community Oriented Policing Services (COPS) and Federal Emergency Management Agency grants in FY2003 and was incorporated in the COPS and the Department of Homeland Security's Office of State and Local Government Coordination and Preparedness (SLGCP) grant processes in FY2004. Included in the grant guidance is the development of a meaningful governance structure that brings together the appropriate parties in the development of a communications solution. SAFECOM believes that such a governance structure, which includes representation of statewide bodies or initiatives, based on a locally driven principle that focuses on the end user needs and requirements, is critical to the success of any communications initiative.

DHS, through the SAFECOM Program, has already partnered with the Commonwealth of Virginia to develop a strategic plan for statewide communications and interoperability. In recognition of the vital input of local practitioners, SAFECOM developed a methodology to ensure local practitioner input into the statewide plan, which will serve as a model for other states and regions developing statewide communications and interoperability plans. To develop this strategic plan, SAFECOM conducted six focus group sessions with local practitioners in diverse regions across the Commonwealth in preparation of a larger strategic planning session held in Richmond, VA. The methodology developed out of the Virginia planning process will be published by SAFECOM as a model for other states developing statewide interoperability plans.

QFR from Congressman Putnam

House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census

September 8, 2004, Hearing

At the same time, the Department's SLGCP required all states to conduct comprehensive needs and vulnerabilities assessments through the State Homeland Security Assessment and Strategy process (SHSAS) in order to receive FY 2004 Homeland Security Grant Program (HSGP) funds. The assessment and strategy development process was a collaborative and coordinated effort between states and local communities, which identified needs and vulnerabilities at the state and local levels. Further, urban areas receiving support under the Urban Areas Security Initiative (UASI) were required to conduct and develop urban area homeland security strategies.

All HSGP and UASI grant funds must be spent according to these strategies. The strategies are preparedness strategies that should be used by the states and urban areas to direct all resources they receive from the federal government or the state to achieve the goals and objectives listed in these strategies. These strategies are reviewed by an interdepartmental group in DHS. Providing funds through the states, along with a strategy framework for spending funds, allows for funds to be effectively coordinated and spent at the state and local level for required equipment, including communications systems. Please see attached for a spreadsheet detailing the HSGP and UASI funds that states have used to support the procurement of interoperable communications equipment since FY 2002.

Lucent Technologies
Bell Labs Innovations

William T. O'Shea
President
Bell Laboratories

600 Mountain Avenue
Room 6C-334
Murray Hill, NJ 07974 USA

Phone 908 582 8541
Phone 908 582 2077
woshea@lucent.com

September 8, 2004

The Honorable Adam Putnam
Chairman
House Government Reform Committee
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
United States House of Representatives
Washington, DC 20515

The Honorable William Lacy Clay
Ranking Member
House Government Reform Committee,
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
United States House of Representatives
Washington, DC 20515

Dear Messrs. Putnam and Clay:

Thank you for holding this hearing today on Spectrum for Public Safety Users. I am writing this letter for inclusion in the official record.

I am the President of Bell Labs, the division of Lucent Technologies that has helped this country address critical communications challenges for over a century.

The Opportunity and Challenge

Lucent believes that we have an historic opportunity to enhance the safety of our nation and its citizens for generations by enabling national responders -- not just the firefighters, public safety officers and emergency medical technicians but also many others who help us every day -- to more effectively draw upon the capabilities of advanced mobile communications networks.

We applaud those who are seeking to develop solutions to the problems associated with voice interoperability. This is vitally important, but while critical, addressing these issues alone will not suffice. It limits our consideration in this critical area to a pre-9/11 context, even though our challenges, and the technologies that are available to meet them, are dramatically different in a post-9/11 world.

National responders should have access to the full range of communications capabilities, particularly broadband and data transmission that are increasingly

commonplace in the commercial and consumer markets. Business users can access company-specific applications, browse the web, download maps and directions and check email while on the road. Even our children can take and send pictures and streaming videos using their cell phones. But most of our national responders, the people we rely on to protect our lives and safety, cannot. And, those who do have such access generally operate at speeds far, far slower than you and I probably do on our home computers. America's first responders need – they deserve – access to the **same technologies** so that they can see where they are going and know what they are seeing each time they respond to an incident, whether it is down the block or across the country.

I am confident that a dedicated, secure, interoperable, nationwide broadband communications network that provides those capabilities can be implemented on a cost effective basis within 24 months using existing commercially available technologies.

Developing and Implementing a Solution

We learned tragically on September 11, 2001, that our national responders lacked adequate communications capabilities. The 9/11 Commission report confirmed this, stating, "inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania, crash sites, where multiple agencies and multiple jurisdictions responded. The occurrence of this problem at three very different sites is strong evidence that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains an important problem." The Commission called for the establishment of a "trusted information network" for our national responders and the provision of "expedited and increased assignment of radio spectrum for public safety purposes." Building upon these two key recommendations, Lucent would like to set out what this trusted national responder information network should look like:

This dedicated, "trusted information network" would serve, for the first time, **all** public safety users – what we call our national responders. Users would include not only traditional law enforcement officers and fire and public safety responders at all levels of government, but also national response plan and national incident management system responders, private sector critical infrastructure owners and operators, health professionals, national security and emergency preparedness decision makers, as well as key municipal officials and military leadership. We estimate this broader national responder group to number between five to ten million.

This "trusted information network" would be available and interoperable nationally, not just regionally or within a particular urban area. This is critical in our ability to enhance daily operations for national responders, and to coordinate a metropolitan, regional or national response to the post-9/11 threats that face us, including biological, chemical, or nuclear threats.

This network would provide secure, interoperable, **broadband** capability, as well as redundant voice communications, to supplement existing voice capabilities and technologies already used by our public safety and national responders. This network can be accessed from commercial or customized handheld or vehicle-mounted devices, and can send, among many things, real-time video, high-resolution images, and geo-spatial data for immediate use by incident commanders during tactical operations.

Lucent Technologies believes that any true public safety interoperability solution must consider both voice and broadband capabilities, and must do so in ways that maximize the efficiencies gained through competition and through partnerships between the public and the private sector.

We would like to make two additional points about this network. First, it would provide significant cost savings to taxpayers. Since this network would use existing commercial standards, large numbers of hardware manufacturers and software developers would be able to enter the marketplace and develop the myriad hardware and software applications the national responder community will want to leverage this next generation of communications connectivity. Using open standards and commercial-off-the-shelf products will not only maximize the cost effectiveness of this network over one based on proprietary, or non-commercial standards, but it will provide end users with maximum flexibility to choose those technology options that best suit their needs. Establishing commercial standards as the platform would additionally drive innovation at lower costs, since a global user base would absorb R&D expenses. Since this network is based on technologies already in commercial use, it can be implemented nationwide for the benefit of our national responders within 24 months.

Second, this network could provide the added benefit of bringing much needed broadband connectivity to millions of American citizens who live in rural areas and who currently have no access to the information highway. This last benefit can only be accomplished with Congress choosing the right spectrum band and sufficient spectrum to achieve this vision.

Finding a Home for the Network

We recognize that one of the challenges facing the Congress is where to find a home for this critical national asset. We believe that the optimal location for this trusted information network would be in the C&D blocks of the upper 700 MHz band. While this spectrum can certainly be used for other applications, we believe the cost benefits to the taxpayer by building a dedicated, national responder network in this band would outweigh any potential auction proceeds. The upper 700 MHz band has significant operational advantages for public safety, and offers significant cost advantages to the taxpayer, because of the lower deployment costs. Fewer towers are needed because upper 700 MHz transmissions propagate more efficiently than transmissions in other bands. Transmissions in the upper 700 MHz band penetrate buildings more easily, a significant problem described at length in the 9/11 Commission's report.

Lucent envisions a dedicated national network that would support the broadband data needs of the national responder community. In major markets, the full 30 MHz would undoubtedly be required to support the national responder base and provide the additional capacity for major emergencies. Lucent envisions, however, that in some geographic areas, portions of the 30 MHz could be leased back to municipalities or commercial entities to provide the rural broadband access that many seek. In essence, a network built to support the national responders' daily activities, and under an all-hazard scenario, could also serve to provide the rural broadband connectivity that many commercial entities seek within this band.

Alternative frequency bands (in particular, the 4.9 GHz band) are being proposed for public safety data requirements. There are several issues that must be understood

with regard to these proposals: 1) the allocation proposed is for the public safety users, and not the extended national responder community; 2) the 4.9 GHz band, as currently envisioned, supports neither the capacity requirements for the public safety community alone, much less the national responder community; and 3) the propagation characteristics at this band do not lend themselves to providing a cost-effective, ubiquitous national network, nor sufficient in-building penetration.

This is not to say this trusted information network vision is not compatible with placement in other portions of the national spectrum, and we welcome the opportunity to discuss this important issue further with the Committee. What is important, however, is that we bring our national responders 21st century communications capabilities, and that the Congress re-consider where the greatest good can be accomplished in determining the spectrum placement for this requirement.

Conclusion

We make these suggestions recognizing that only Congress can ultimately address where the greater public good and necessity is met and how the safety of the public can be accomplished in a manner justifiable to our ultimate constituency -- the American citizens. We have served and advised this country for more than 100 years, and we believe Congress has a unique opportunity to consider how best to provide a trusted information network that can be used by all national responders. This is an historic opportunity to enhance the safety of our nation and its citizens for generations.

Thank you for the opportunity to include these comments in the record. We would welcome the opportunity to answer any questions that you or other members of your committee might have.

William T. O'Shea

○